PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 :
H04Q 11/04

A1

(11) International Publication Number: WO 99/14979

(43) International Publication Date: 25 March 1999 (25.03.99)

(21) International Application Number: PCT/US98/19096

(22) International Filing Date: 14 September 1998 (14.09.98)

(30) Priority Data:

60/058,875	15 September 1997 (15.09.97)	US
09/149,422	8 September 1998 (08.09.98)	US

(71) Applicant: SECANT NETWORK TECHNOLOGIES [US/US]; Suite 300, 951 Aviation Parkway, Morrisville, NC 27560 (US).

(72) Inventors: WINKELSTEIN, Daniel, R.; 2308 Lawrence Drive, Raleigh, NC 27603 (US). STEVENSON, Daniel, S.; 4 Fallen Oak Court, Durham, NC 27713 (US). HILLERY, Nathan, H.; 904 Queensbury Circle, Durham, NC 27713 (US). BYRD, Gregory, T.; 105 Durington Place, Cary, NC 27511 (US).

(74) Agent: SAVAGE, Michael, G.; Burns, Doane, Swecker & Mathis, L.L.P., P.O. Box 1404, Alexandria, VA 22313–1404 (US).

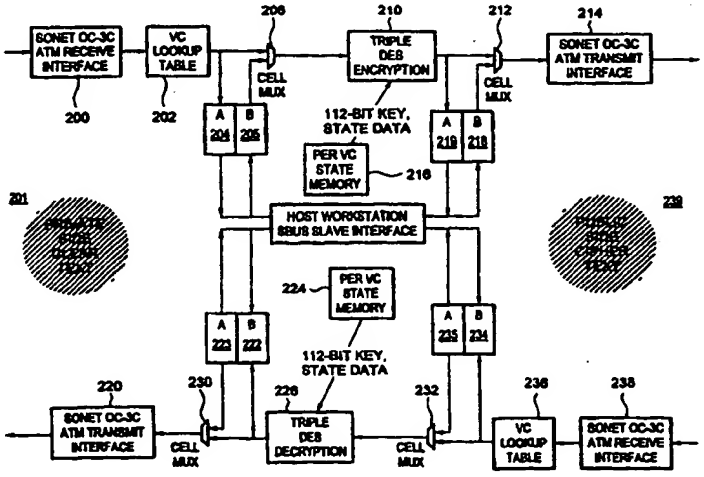
(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, GM, HR, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published

With international search report.

Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: CRYPTOGRAPHIC SYSTEM FOR PUBLIC ATM/SONET COMMUNICATION SYSTEM WITH VIRTUAL CIRCUIT LOOKUP AND PIPELINED DATA ENCRYPTION AND DECRYPTION



(57) Abstract

A communications system employing sending and receiving cryptographic units provides transparent security for digital communications in Asynchronous Transfer Mode Networks. Each cryptographic unit is placed between the untrusted network and a secure host or LAN. The cryptographic unit replaces the cleartext packet with encrypted text, and manages all keys between sender and receiver so as to be transparent to the user. Plural virtual circuits, each with distinct cryptographic state information, are processed in real time. Packet cryptographic processing time is reduced by ordering a list of active virtual circuits and using a binary search to lookup cryptographic state information for each virtual circuit. In addition, triple DES encryption and decryption is implemented in a pipelined data flow architecture using multiple FIFO storage for algorithmic key agility permitting both triple and single DES operations using the same cryptographic unit.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

CRYPTOGRAPHIC SYSTEM FOR PUBLIC ATM/SONET COMMUNICATION SYSTEM WITH VIRTUAL CIRCUIT LOOKUP AND PIPELINED DATA ENCRYPTION AND DECRYPTION

Background

The present invention relates to the field of cryptographic communication. More particularly, the present invention relates to methods and apparatus for transparent security on cell bused switched networks such as Asynchronous Transfer Mode (ATM) carried on a digital public switched telephone network.

Information transmitted by business, individuals and institutions over public, local, and wide area networks often represents valuable confidential information, such as trade secret data, patentable inventions or copyrightable software. Information transmitted over a non-secure network can be intercepted by third parties and be the subject of theft or tampering. It is desirable to provide a security system to encrypt such information as a precaution against third party access.

A non-secure communication system may have a security system overlay. For example, analog audio scrambling devices, which attach to a telephone connection at each end, are available for scrambling telephone conversations over standard telephone systems. Encryption systems for data are also known, such as those used to encrypt satellite transmitted data. A typical security system comprises a pair of cryptographic units and a management system, which includes a key management system for exchanging cryptographic keys between a pair of cryptographic units. Each cryptographic (crypto) unit is located between a secure host or local area network and the non-secure public network. A calling party is coupled through a first cryptographic unit (crypto unit) to the non-secure network. A second crypto unit is placed at the far end between the non-secure network and the called party. The first and second crypto units encrypt information before transmission over the non-secure network and decrypt information after reception from the non-secure network between the called and calling parties. In such manner, a cryptographic overlay provides secure communications between the calling and called parties over a non-secure network.

Public networks use several types of standard forms of signaling protocol. In particular, voice, video and data traffic are transmitted using industry standard asynchronous transfer mode (ATM) and synchronous optical network (SONET) protocols. Public wide area networks are now available using standard communications protocols provided by common carriers, such as the local telephone companies. Favorable prices for such standardized public communication services are due to the economy of scale resulting from extremely large numbers of connections and high levels of traffic.

Instead of using the public networks, telephone companies have in the past provided private

links in order to create a private wide area network. A private wide area network is not inherently any more secure than a public network because the private network provided by the telephone companies merely ensures that no one else is sharing the private resource. Thus, the use of a private network does not prevent wiretapping (either authorized or unauthorized) any more than a public network because a private network is still accessible to an attacker. However, one of the consequences of the emerging ATM network technology standards is that the price-performance ratio of standardized commercial service providers using ATM/SONET technology is more cost effective compared with private wide area networks.

Nor can the standards used by public networks be easily modified to incorporate security. Modification of standard networks can be made only through a lengthy standards process, which is beyond the control of individuals, corporations and institutions interested in implementing a security overlay architecture. For the above reasons, it is desirable to provide a cryptographic system with connection management system compatible with the public network specifications so that a security overlay system will be adapted to work with existing standard high performance ATM/SONET networks.

Summary

A pair of crypto units are placed at the respective near and far boundaries of a public ATM/SONET system between the untrusted public network and a pair of secure hosts or private LANs. At each end, the crypto unit replaces the cleartext transmitted packets with encrypted text, decrypts the received encrypted packets, and manages all keys between sender and receiver so that the crypto units are transparent to the users. Encrypting data packets makes communication over the public networks more secure against unauthorized access to information by a hostile third party.

A virtual circuit (VC) is an apparent connection through the public network, which gives the impression to the user of a continuous end to end connection. The key agile cryptographic overlay system of the present invention is able to handle plural independent VCs between different senders and receivers, and unique cryptographic keys for each VC. Key update provides additional security by providing the means to change keys for a VC while it is active. Algorithm agility avoids the need for different types of crypto units by providing a plurality of encryption algorithms in one crypto unit.

To implement a secure encryption system in an ATM network, a VC number is passed along with each encrypted packet as cleartext in a header field from the transmitting side to the receiving side. The VC number is assigned as part of the link level protocol in the ATM system. In general, for a given virtual circuit connection, the VC number at the transmitting side is the same VC number from one ATM cell to the next ATM cell corresponding to the same virtual circuit. Similarly, at the

receiving side, the VC number is the same from one ATM cell to the next ATM cell corresponding to the same virtual circuit. However, the VC number at the transmitting side is, in the general case, not the same as the VC number at the receiving side. Thus, a pair of VC numbers is associated with each virtual circuit, and the pair of VC numbers does not change for the duration of a given virtual circuit connection.

At the transmitting and receiving end, cryptographic state information is stored corresponding to a given virtual circuit. The cryptographic state information includes keys and initial vectors, which allows the crypto unit to pick up the encryption/decryption process where it left off since the reception of the last received/transmitted packet for the same virtual circuit. At the transmitting end, cryptographic state information is retrieved from memory and used to encrypt an outgoing ATM cell payload. At the receiving end the same cryptographic information is retrieved from memory and used to decrypt the incoming ATM cell payload. A single crypto unit has the cryptographic agility to handle a large number of multiple virtual circuits, with limited lifetime keys, using either single DES or triple DES.

Plural virtual circuits, each with distinct cryptographic state information, are processed in real time. It is desirable to process received or transmitted packets through the crypto unit as quickly as possible to reduce the delay caused by encryption and decryption, which contributes to the total network latency. Packet cryptographic processing time is reduced by using a rapid virtual circuit lookup implemented in hardware, and a pipelined data flow for high-speed triple DES implementation. The present system has a high degree of algorithmic agility, permitting both triple and single DES operations using the same cryptographic unit.

VC LOOKUP CIRCUIT

A VC lookup circuit retrieves the previously saved cryptographic state information relating to the current ATM packet. The retrieved cryptographic state information is used to prepare an encryption/decryption engine to process the next packet. The incoming ATM data packet contains a VC number representing the virtual circuit to which it belongs. The task of the VC lookup circuit is to retrieve the cryptographic state information from memory corresponding to the VC number of the incoming ATM data packet. Implementing a VC lookup circuit is a problem. On one hand, if the system provides for only a small number of VCs, a VC lookup circuit can readily be implemented, even entirely in software. However, providing for only a small number of possible virtual circuits limits the capacity of the network to support traffic growth.

It is desired to provide for a large number virtual circuits, for example, up to 65,535 virtual circuits. To provide for 65,535 virtual circuits, the cryptographic state information for the 65,535 possible virtual circuits is stored in a 28 bit memory address space. The address range of 2^{28} is

greater than 256 million addresses. The VC lookup implementation attempts to find the specific cryptographic state information associated with one of 65536 supported VCs given the VC number space is 256 million possible values. The available time interval to find the cryptographic state information associated with a packet is based on the speed of packet framing, or 2.8 microseconds in the case of ATM/SONET at OC-3c rates. In such case, the VC lookup circuit completes its search 2.8 microseconds or less including the time to use the cryptographic state information to place the crypto unit in a condition to receive the next ATM data packet.

To speed up the VC lookup search, a special binary search method is implemented. First, prior to the search, an ordered list of active virtual circuits is created and stored in a small, fast static RAM memory. The VC list is stored in order of VC number. The ordered VC list requires reordering and updating of the list whenever a new VC is opened. To lookup a VC, the list in RAM memory is accessed at the midpoint, and the contents compared to the incoming VC. The address at the midpoint of the RAM memory is presented to the RAM memory; the output is the VC number at that address. If the VC returned by the RAM memory is greater than the VC of the received cell, the next address presented to the RAM memory is at the 1/4 position in the RAM memory. If the VC returned by the RAM memory is less than or equal to the VC of the received cell, the next address presented to the RAM memory is at the 3/4 position. The search cycles 16 times, where for each cycle the VC returned by the RAM memory is compared against the VC of the received cell, and the address presented to the RAM memory is adjusted up or down by 1/2 the remaining unsearched address space.

The search of the ordered list is completed in 16 cycles for 65,536 (65K) active VCs. If the cell has an entry in the VC lookup table, an index (address) to the state is returned. The retrieved index is used to get the cryptographic state information from an exact position in a larger DRAM memory space.

PIPELINED TRIPLE DES

The cryptographic state information provides cryptographic keys and initialization information for the DES processing engine. Like the VC lookup task, the available time interval for the DES processing engine to encrypt or decrypt an ATM data packet, in time to be ready for the upcoming ATM data packet, is based on the speed of packet framing, or 2.8 microseconds for OC-3c. In such case, it is desirable that the DES complete its encryption or decryption in 2.8 microseconds or less, including the time to place the DES processing engine in a condition to receive the next ATM data packet.

High-speed DES chips implemented in gallium arsenide (GaAs) is known. However, such GaAs chips are expensive, require high power, special cooling and utilize a relatively large amount

of board space. Less expensive conventional chips are available, but are not fast enough to complete DES processing time within one packet frame. The cryptographic unit of the present invention uses slower, less expensive DES chips in a pipelined (data flow) DES engine with multiple FIFOs. The pipelined DES architecture permits the use of slower DES chips, which are less expensive to buy and to use in a DES processing engine.

In order to use slower chips, a plurality of pipelined triple DES circuits and a plurality of FIFOs are used to store and process incoming ATM data packets in a round robin fashion. Each FIFO and pipelined DES circuit works in parallel to complete triple DES encryption or decryption in a multiple of ATM packet frames. In such manner, the parallel arrangement of the present invention allows slower DES chips to perform DES encryption or decryption at an aggregate speed fast enough to keep up with the speed of the incoming ATM cells.

Brief Description of the Drawings

Figure 1 is a block diagram of a communication system utilizing a cryptographic unit in accordance with the present invention.

Figure 2 is a block diagram of a cryptographic unit in accordance with the present invention.

Figure 3 is a block diagram illustrating the interface of the present invention to the public switched network.

Figure 4 is a block diagram of a virtual circuit (VC) lookup apparatus in accordance with the present invention.

Figure 5 is a flow chart of a VC lookup method in accordance with the present invention.

Figure 6 is a block diagram illustrating Counter Mode used in conjunction with the present invention.

Figure 7 is a block diagram of the state memory circuit on the encryption side in accordance with the present invention.

Figure 8 is a block diagram of a pipelined triple DES circuit in accordance with the present invention.

Figure 9 is a timing diagram illustrating the staggered timing of data and key loads for the pipelined triple DES circuit of Figure 8.

Figure 10 is a block diagram overview of crypto unit using two pipelined triple DES circuits.

Figure 11 is an embodiment of the encryption controller, 706, 718 of figure 8 configured to use a pipelined triple DES encryption/decryption engine with either Electronic Code Book (ECB) or Counter Mode.

Figure 12 is a timing diagram illustrating the data input output for the triple DES encryption circuit of Figure 11.

Detailed Description

The present security system provides protection at the boundary between each of the distributed components of a secure network and the non-secure network. Figure 1 shows a network 22 with the present security system overlay 21 implementing security at a plurality of endpoints. As equipment is added to the system to create a new endpoint, additional equipment is added at the endpoint as a security mechanism to secure the new endpoint of the expanded network.

Endpoint equipment, compliant with the ATM user-network interface specifications, is supported without modification. Hosts 10, 28, are devices which serve as the endpoints of ATM connections. Hosts are usually computers, though the architecture of the security system or crypto unit supports the attachment of other kinds of ATM devices. Secure hosts 10, 28, as well as secure private LAN 26 and secure ATM terminal 14 are the entities for which security services are provided by crypto units 14, 24, and 16 respectively. Non-secure hosts 18 are those devices that exist outside the domain of the security system.

The security system, in conjunction with a certificate authority 20, will enforce access control for host communication across the untrusted network 22. Connection establishment requests from a host are intercepted and interpreted, and the requested connection checked against an access control list. If the requested connection is allowed, then the connection establishment message is passed on to the network. Otherwise, the message is dropped and a reply sent to the host indicating the connection could not be established. A similar action takes place when a party is added to an existing point-to-multipoint connection.

OPERATION - ACCESS CONTROL AND AUTHENTICATION

The security management system holds security policy information such as access control lists and conducts audit functions. The managers of the security system develop various rules about which hosts may access other hosts and resources. Information about access control is contained in the management system and is distributed to the crypto units 16, 14, 24 for enforcement. When a connection release request is received, the resources associated with the call that are reserved in the security system are released at the same time that the channel is released.

A reliable authentication function is required between the various elements of the cryptographic system. Assumptions about the nature of authentication methods are based on information in the open literature on public key cryptography systems and protocols for authentication. A two-way authentication exchange between crypto units precedes each key distribution and is carried out before establishing each new secure virtual connection.

SECURITY AND KEY MANAGEMENT

There are several basic crypto unit management functions. Management functions include monitoring system status and performance, modifications to security policy parameters and access control data, and downloading and statistically analyzing audit data. For small groups of crypto units managed by a single organization or company it may be possible to undertake these system management functions locally. However for large collections of crypto units under a centralized management, system structure is provided to remotely perform these functions over the network in a secure manner that does not result in opportunities for system compromise.

Key management is a critical cryptographic function. Key management functions include generation and distribution of keys. The primary responsibility for key management is distributed to the crypto units. Security policy provides for a unique key for each connection and limited key lifetimes. Consequently, a unique key is negotiated for each secure point-to-point or point-to-multipoint session over the untrusted network. The system design supports policy based setting of key lifetimes, which may be shorter than the holding time of at least some connections, resulting in dynamic key updates during established sessions.

CRYPTO UNIT

A crypto unit is a device that serves as the interface between a trusted ATM host or network and an untrusted ATM network. A prime system objective is that crypto units are transparent enough to be merely minor delays in most situations. Crypto units provide the mechanism for intercepting connection management messages and taking actions based on the message contents, the originating host, the destination host, and the security policy. Once a connection is established, data is passed between end hosts by way of one or more crypto units. In accordance with security policy guidelines, data within a given connection may or may not be encrypted for privacy during transit of the untrusted network. For secure calls, a crypto unit at the destination will receive and decrypt the data and pass the plain text data on to the destination.

A crypto unit also is capable of proving its identity to other system elements. To establish its identity, each crypto unit has a crypto unique ID value established in a registration process. Registration is performed in a trusted environment and results in a public key certificate that establishes an association between the crypto ID and its public key. Additionally, for secure key management communications crypto units will need the capability to send and receive messages encoded under another cryptographic method. Communication between crypto for key management uses a small bandwidth, and a more computationally intensive algorithm.

The crypto unit is placed between a trusted (private) network and untrusted (public) networks. The crypto unit is transparent to the user. There is a small hardware latency for encryption

and decryption of cells. Hardware latency for encryption and decryption of cells is less than 20μs.

The security system operates in the following sequence:

1.) When a user requests a virtual circuit, the system crypto unit intercepts the call processing signaling messages from the user.

2.) The security system then sets up a virtual circuit (VC) between encryption units. This setup involves both network setup and the exchange of keys between crypto units. Once the virtual circuit is setup between crypto units, it is extended to the end-user.

3.) Once the call has been setup, the security system accepts ATM cells for the virtual circuit. The payload of each cell is encrypted using triple DES and a unique key (session key) for this VC. The payload of the ATM cell is 48 bytes, divided into 6 blocks, each having 64 bits (8 bytes) per block.

4.) At the far end of the network, the cell payload of the VC is decrypted and clear-text data is passed to the destination.

5.) Based on policy, the security system allows the session key to be changed at any time.

Each security system handles in hardware the encryption requirements for up to 65,535 unique virtual circuits, with each virtual circuit having a unique encryption key. The security system uses triple DES encryption techniques for encrypting the data (112-bit key encryption on 64-bit blocks). On a per-VC basis the system supports triple DES Electronic Code Book Encryption (ECB) and ATM Forum specified Counter. The hardware on the crypto unit board allows the system to intercept or generate signaling messages and crypto-to-crypto messages.

Figure 2 illustrates the operation and data flow of the ATM crypto unit. The SONET OC-3c ATM interface 200, 238 receives ATM traffic on OC-3c SONET links. The interface on the trusted side 201 may be multimode fiber or single mode fiber while the interface on the untrusted side 239 will usually be single mode fiber (but it can be multimode). On the receive side, this circuit performs SONET clock recovery, performs line, section, and path overhead processing, and extracts the ATM cells from the SONET payload. ATM cells received on the trusted side 201 are passed to a VC lookup table 202. The VC lookup circuit compares the virtual circuit identifier (VCI) of each cell with the list of active VCs, using all 28-bits of VPI/VCI address space for the search. (For UNI traffic, the GFC field must be set to zero; the VC lookup circuit treats all VCs as formatted for NNI with a 12-bit VPI space and a 16-bit VCI). The output of the VC lookup table 202 is an index and a set of flags associated with that VC. The index indicates which of the 65,535 active virtual circuits corresponds to the received cell. The flags indicate if the cell is to be passed to the crypto host via the receive FIFO or sent to the encryption circuit. Other flag information includes type of encryption, valid index, and clear text. If a cell arrives whose VC is not in the list of active virtual

circuits, the cell is discarded.

The VC lookup table 202 uses a binary search technique to improve processing time. There is a time constraint that each encrypted ATM cell must be processed before the next ATM cell arrives. Accordingly, techniques to speed up operation are important. The binary search technique for VC lookup is discussed further in conjunction with figures 4 and 5.

Signaling messages and crypto-to-crypto messages are intercepted after the VC lookup table circuit and passed to the host via the receive FIFO 204. All active virtual circuits are passed to the cell multiplexer 206. For simplicity of design, all received virtual circuit information is treated alike; non-active virtual circuits are discarded later. The receive FIFO 204 is 4Kbytes deep and is accessed by the host. The host can also insert data into the traffic stream by writing data to the transmit FIFO 205 (which is also 4Kbytes deep). An ATM cell multiplexer 206 will pass all active virtual circuits. When an idle (or unassigned or non-active VC) cell is received, the cell multiplexer 206 may insert a cell from the transmit FIFO 205.

The encryption circuit 210 uses the index associated with the VC to access a state memory table 216. The state memory table 216 contains the encryption keys for that VC, State Vector for Counter Mode and some dynamic flags. The keys for that VC are loaded into the triple DES circuit 210. The cryptographic state information retrieved from memory table 216 allows the crypto unit to pick up the encryption/decryption process where it left off since the reception of the last received/transmitted packet for the same virtual circuit. All dynamic information (data that changes on a per cell basis) is held in the state memory table. All static information (data that changes only when a VC is setup or taken down) is held as part of the VC lookup table. The triple DES encryption circuit 210 performs three different types of encryption based on flags retrieved from the VC lookup circuit 202: 1) No encryption - data passed as clear text; 2) Electronic code book; and 3) Counter Mode. VCs using Counter Mode require periodic synchronization. For encryption methods with significant error extension, synchronization is used as a means of restoring crypto units to known states of operation. The required rates of synchronization events are related to transmission efficiency.

The encryption circuit 210 passes the ATM cell header transparently and encrypts the payload of the ATM cell. Since each VC has a different key, the keys are loaded dynamically into the triple DES circuit 210. Each cell time, the key (if single DES) or keys (if triple DES) for the next cell are loaded into the triple DES circuit prior to the arrival of the cell data. The triple DES circuit 210 is pipelined to allow the use of slower, less expensive DES chips. The pipelined DES encryptor (or decryptor) is discussed in further detail in conjunction with Figures 9-12.

The encrypted data is then passed to a second FIFO/multiplexer circuit 218, 219, 212. This

circuit allows encrypted cells to be extracted and passed to the host. This feature allows the board to do small amounts of hardware accelerated encryption for the host. The transmit FIFO allows the host to insert cells into the outgoing data stream. The SONET ATM interface 214 on the public side 239 transmits the ATM cells over SONET at OC-3c rates over single-mode or multimode fiber.

The decrypt circuit (220 through 238) is nearly identical to the transmit circuit with the exception that the triple DES circuit 226 is set for VCs using ECB. Crypto-to-crypto messages are received either before or after the decryption using receive FIFOs 234, 222. Call setup messages back to the user are transmitted by writing the data to the transmit FIFO 223 on the trusted side of the decryptor. The decrypt circuit 226 allows hardware acceleration of decryption using the transmit FIFO 235 and cell multiplexer 232 on the cipher text side 239 of the decryptor 226 and the receive FIFO 222 on the clear text side 201.

Figure 3 illustrates the operation and data flow of the ATM crypto unit. The untrusted side 302, 303, 304, 306 network interface is 155.08Mbps single mode fiber (which can be alternatively configured as multimode fiber). The trusted side 308, 310, 312, 314 network interface is 155.08Mbps multimode or single mode fiber. The receive side of the SONET interface performs opto-electronic conversion, clock recovery, SONET framing and cell formatting. The transmit side of the SONET interface formats cells into SONET frames, and performs opto-electronic conversion.

The opto-electronic receivers 302, 308 and transmitter 303, 310 circuits receive and transmit data as differential PECL signals. For the single mode interfaces the HPCDX1155B transceiver module is used, for multimode fiber the HFBR-5205T transceiver module is used, both available from Hewlett Packard Company, Palo Alto, California. These modules are pin-for-pin compatible and fit in the industry standard 1X9 form factor, allowing flexible use with either the single mode transceiver or the multimode transceiver.

The clock recovery circuit 304, 312 is the Cypress CY7B951 clock recovery circuit. This device recovers clock from the received data and outputs the clock and data to the ATM interface chip. The ATM interface circuit 306, 314 consists of the PM5345 SUNI SATURN Interface device from PMC-Sierra of Vancouver, British Columbia, Canada, which implements the SONET processing and ATM mapping functions for 155 Mbps ATM networks. The SUNI device has an 8-bit processor interface that is accessible to the host via the host interface circuit. The receive ATM interface internal to device 306, 314 consists of an ATM cell FIFO. The internal ATM FIFO provides a cell present signal. The interface to the SUNI formats the ATM cell into a 64 byte cell by pre-padding the cell with an 11-byte crypto unit header. When a cell is present on the ATM receive interface of the SUNI, the crypto unit formatting circuit extracts the cell on a 23 MHz system clock. This clock is slightly faster than the cell rate for a full OC-3c synchronous payload envelope

(including SONET frame slippage). This means that periodically the cell FIFO will be empty. When the cell FIFO is empty, the crypto unit interface inserts an unassigned cell into the cell stream. The extra bandwidth is used for hardware acceleration of encryption functions in crypto-to-crypto key-exchange.

On the transmit side, the crypto unit formatting circuit removes the 11-byte crypto unit header, checks if the cell is valid (described below), and if so, inserts the cell into the transmit side ATM interface. This interface is a FIFO, so cell data is written into the FIFO on a 23MHz clock. If an invalid cell is present, it is discarded prior to insertion into the data stream. If the ATM FIFO on the SUNI is empty, the device inserts an IDLE cell into the outgoing data stream. The transmit side timing for both the trusted and untrusted side may be slaved to the receive side timing on the untrusted side of the network to ensure proper distribution of SONET clock timing. The crypto unit is plugged into the untrusted (public) network.

The cryptographic system is comprised of custom cell encryption hardware (a crypto unit) and key management software, both operating within an embedded computer. The embedded computer is a Sun SS20 or Sun Ultra 140, running Solaris 2.5.1 or higher. The encryption system supports ATM cells over SONET at OC-3c rates, and is adaptable to support ATM over T3 and T1 interfaces. Each crypto unit supports full duplex encryption.

OPERATIONAL SPEED

In order to operate at ATM/SONET speeds, each crypto unit must store the ATM cell, look up cryptographic state information for the VC, and initialize a DES encryptor (for transmit) or a DES decryptor (for receive) to be ready for active use before the cell payload arrives. At the same time, while processing an ATM cell, triple DES encryption and triple DES decryption is performed at ATM/SONET clock rates.

VIRTUAL CHANNEL LOOKUP

The crypto unit supports up to 65,535 simultaneous virtual circuits. The VC lookup circuit (one for each direction, 202 and 236 in figure 2) provides a mapping between the received VPI/VCI and an index associated with each of the active virtual circuits. The problem is that each of the 65,535 active VCs can be anywhere in the 2^{28} = 268,435,456 element VC space. Figure 4 is a block diagram of a VC lookup circuit.

Consecutive ATM cells arrive every 2.8 microseconds for OC-3c rates (705 nanoseconds for OC-12c rates). The cell is buffered in a memory (416 of figure 4), while the header which contains the VC number is copied into a comparator circuit 402. The function of the VC lookup circuit is to find an index corresponding to the VC number. The index is a pointer to a memory location in DRAM that contains the state of the encryption or decryption process since the last cell

corresponding to the same VC.

As previously indicated, the problem in retrieving the index arises because the VC space for ATM cells is very large (namely 2^{28} or 268,435,456 entries). It is necessary to find the state data associated with each VC in a small amount of time (less than 2.8 microseconds for OC-3c and less than 705 nanoseconds for OC-12c). The present VC lookup arrangement supports a very large number of active concurrent VCs (65,536). At the same time, the VC lookup arrangement is scaleable to support substantially more VCs, wherein support for more VCs does not require a substantial increment in the time to search for the state data, or impose any limits to the size of the search space.

Solutions to the VC lookup problem include content addressable memories (CAM), or a restriction on the VC space, or both. Current technology in CAMs limits the number of active VCs for use in a CAM to less than 4096 active circuits. A transparent security device cannot restrict the VC space and remain transparent. Yet another solution is an exhaustive linear search, which is unacceptably slow and does not scale well. A third approach is a complete lookup table of 2^{28} possible entries. The preferred solution in the present invention is to prepare an ordered list of VCs in advance, and use a binary search to traverse the previously ordered list of VCs. The following steps are performed by the hardware each cell time (2.8 microseconds for OC-3c).

1.) The hardware receives the ATM cell and stores the VC of that cell.

2.) The address at the midpoint of the RAM is presented to the RAM; the output is the VC number at that address.

3.) If the VC returned by the RAM is greater than the VC of the received cell, the next address presented to the RAM is at the 1/4 position in the RAM. If the VC returned by the RAM is less than or equal to the VC of the received cell, the next address presented to the RAM is at the 3/4 position.

4.) The search cycles 16 times where each cycle the VC returned by the RAM is compared against the VC of the received cell, and the address presented to the RAM is adjusted up or down by 1/2 the remaining unsearched address space.

The search is complete in 16 cycles for 65,535 active VCs. The search cycle may be truncated by exiting after detecting equality between the VC of the received cell and the VC returned by the RAM memory. However, the search logic is simplified by using a regular 16 cycle search regardless of whether equality is detected during one of the 16 cycles of the search. If the cell has an entry in the VC lookup table, the index to the state is returned. The retrieved index is used to get the cryptographic state information from an exact position in a larger DRAM memory. If the cell is not present in the VC lookup table, a NULL index is returned. Cells with NULL indexes do not have state information available in the larger DRAM memory. NULL cells are eventually discarded

by the SONET OC-3c ATM transmit I/F circuit (214/220 in figure 2).

A block diagram of the VC lookup circuit is shown in figures 4 and 5. The index is stored in static RAM, 408 or 410 in the form of an ordered list. In particular, the list is in the order of the VC numbers. The VC lookup circuit performs a binary search of VCs stored in the ordered list. When a new virtual circuit is established, the list is reordered to include the new VC. For purpose of reordering the list, Figure 4 has two static RAMs 408 and 410. One RAM is used as the active RAM. When a new virtual circuit is established, a new ordered list is generated to account for the new index number assignment. The new ordered list is stored in the other RAM. The RAMs are swapped in response to an input signal on control line 413, which operates multiplexers 404, 406, 412 and 414 to switch either Ram 408 or RAM 410 as the active RAM.

In figure 4, the input VC from the cell header is one input to comparator 402. The other input is the VC stored in the selected one of the static RAMs 408 or 410. A binary search of 65,535 entries in the table stored in RAM memories 408 or 410 takes a maximum of 16 operations of three 44 nanosecond clock cycles each (48 clock cycles). Once a match is achieved, the 16-bit index associated with the VC, along with some flags, is placed in the header of the ATM cell.

The address used to start the binary search cycle is 0x8000. Depending on whether the VC at that address is greater than or less than the received VC, the next cycle of the address presented to the RAM is either 0xC000 or 0x4000. The third cycle, the address is any one of 0xE000, 0xA000, 0x6000, or 0x2000, and so on until after 16 cycles, every possible memory location will have been checked. The process is illustrated in block form in figure 5. The received VC is stored in a register 510. The stored VC in the fast RAM 516 is compared to the received VC in register 510 in comparator 512. Depending whether the received VC is greater than or less 513 than the stored VC, a next address is calculated 514, and so on for 16 cycles. The full 16 cycle search is carried out, even if the stored VC in RAM 516 at any address is equal 515 to the received VC in register 510. Instead of terminating the search, equality is determined after all 16 cycles, simplifying the design of the VC lookup search logic.

When a new VC is to be added or dropped from the ordered list, the host regenerates the entire list to reflect the new order resulting from the addition or deletion. In order to support host access to reorder the list, while at the same time perform binary searches for VC lookup, the ordered list of active VCs is duplicated in two memories. One list available to the host in memory 408 or 410 and the duplicate list is available in memory 410 or 408, for binary searches. When the host completes re-generation of the list to add or delete a VC, the memories 408 and 410 are switched via control line 413. Control line 413 operates multiplexers 404, 406, 412 and 414 so as to select one of RAM 408 or 410 for active use in binary searches (vial multiplexer 414) and the other for

host access to reorder the stored list (via multiplexer 412).

The lists 128Kx32 bit static RAM (408 and 410 in figure 4) and are formatted with virtual circuits in even addresses and the associated index and flags in odd addresses. All VC entries are in ascending numerical order. The index is an arbitrary (non-zero) 16-bit value that is used to reference the key and state data in the DRAM memory. Index zero is not used for an active VC. The index zero is reserved for operation on invalid cells. The flags indicate the following information:

1.) Valid VC. This bit must be set for all active VCs. For invalid VCs this bit is reset and the cell is discarded downstream.

2.) Extract all cells prior to encryption/decryption. This bit is set if the cell is to be extracted from the data stream and sent to the host prior to passing through the encryption circuit.

3.) Extract OAM cells (Operation, Administrative and Maintenance) prior to encryption/decryption. If this bit is set, then OAM cells are extracted from the data stream and sent to the host prior to passing through the encryption circuit.

4.) Extract all cells after encryption/decryption. This bit is set if the cell is to be extracted from the data stream and sent to the host after passing through the encryption circuit.

5.) Extract OAM cells after encryption/decryption. If this bit is set, then OAM cells are extracted from the data stream and sent to the host after passing through the encryption circuit.

6.) Counter Mode. This bit is set if the encryption method is Counter Mode and is clear if the encryption method is Electronic Code Book or clear text.

7.) Clear text. If this it is set, the VC is not to be encrypted/decrypted and the cell is to bypass to encryption circuitry.

8.) AAL type. For Counter Mode, the encryption process is slightly different for AAL1 and AAL3/4, and AAL5. The following table illustrates the use of these bits.

AAL TYPE	FLAG BITS
AAL0, AAL2	00
AAL1	01
AAL3/4	10
AAL5	11

9) CBC: Cipher Block Chaining, reserved for future use.

Receive 204, 219, 222, 234 and transmit 205, 218, 223, 235 FIFOs and cell multiplexer circuits are provided on both sides of the encryption/decryption circuit. The purpose of the circuits is to extract cells from the ATM stream passing them to the host via a FIFO, and to insert ATM cells into the stream, from the host via a FIFO.

The receive FIFO is 4Kbytes deep. When a cell arrives with the "Extract VC" flag bit set, the 64-byte cell is written into the receive FIFO. Downstream from the receive FIFO is the cell multiplexer circuit. If a cell has been extracted, the multiplexer circuit will change the valid bit to invalid and change the index to the invalid index. If the host has written a cell into the transmit FIFO, the cell multiplexer circuit will wait until a cell arrives with an invalid flag bit set and overwrite that cell with the first cell in the transmit FIFO. It is in this circuit that the crypto unit takes advantage of the fact that the internal cell stream is slightly faster than the cell stream on the ATM link. Thus even if the link is fully occupied, the host can still insert cells into the data stream prior to encryption/decryption and then extract them after encryption/decryption. The higher internal clock allows hardware acceleration of data encryption functions necessary for crypto-to-crypto communication. If the host attempts to insert data for transmission into a completely full ATM stream, the SUNI may discard a cell at random. The total bandwidth available in excess of the ATM data stream is about 2.1Mbps.

STATE MEMORY CIRCUIT

Downstream of the VC lookup circuit, and prior to insertion into the triple DES encryption/decryption circuit, the cell is processed by the state memory circuit. This circuit associates the keys, Counter Mode State Vectors, counts, and alternate keys (for key update), and dynamic flags. For each of the 65,535 active VCs the following information is associated with index found in VC lookup.

1.) Two active DES keys for triple DES operation (112 bits not including parity bits). Note that for triple DES operation with two keys, ENCRYPT operation is Encrypt-Key 1, Decrypt-Key 2, Encrypt-Key 1, while the DECRYPT operation is Decrypt-Key 1, Encrypt-Key 2, Decrypt-Key 1.

2.) Counter Mode State Vector. The Counter Mode State Vector is a 64 bit non-repeating initial vector (IV) used in Counter Mode to create the key stream. For AAL0,2 and 5, the State Vector is changed each cell. For AAL1,3 and 4, the State Vector is changed each time the sequence number in the cell payload cycles.

3.) Cell count. The cell count is a 32 bit count of the number of cells that have passed through the encryption/decryption circuit associated the current VC. The cell count value is incremented for each cell of this VC.

4.) Active key bank flag. Indicates whether the active keys or the alternate keys are to be used for encryption. This key is changed whenever a change occurs in the bank field of any Changeover Cells. (SKC cells are special OAM cells used to synchronize Counter Mode and change key banks.)

5.) Two alternate DES keys, for triple DES. The alternate DES keys replace the active keys when a new key event occurs.

When a cell is received, the State Memory circuit buffers the cell and extracts the index (derived in the VC lookup circuit). The index is used as the address to the state memory. The state memory circuit from the memory the DES keys, Counter Mode State Vector, cell count and flags as follows:

Description	Size (bytes)
Key1	8
Key 2	8
flags	4
State Vector	8
Alternate key 1	8
Alternate key 2	8
counter	4

The above information is held in a 4Mbytes DRAM memory with fast page capability for istorage and retrieval. Figure 7 illustrates the operation of the state memory circuit on the encryption side. When a cell is received, the state memory circuit buffers 502 the input cell and using the VC lookup technique described with regard to figures 4 and 5 above, extracts the index 512. The index 512 is used as the address to the state memory 514. The state memory circuit reads from the state DRAM memory 514 the DES keys (active and standby), the Counter Mode State Vector, a cell count (number of cells for this VC) and flags. The Counter Mode State Vector is updated 520, the cell count is incremented 522 and, if a new key event occurs, the flags are updated. These updates are stored back into the DRAM memory 514. The Counter Mode State Vector, keys for encryption, flags (the formatted key data 518) and the ATM cell data 502 are then multiplexed together and alternately stored in one of two FIFOs 508, 510 which go to independent triple DES circuits.

In particular, the output of the cell data buffer 502, which is alternately loaded into FIFO A cell data (508 in figure 7) or FIFO B cell data (510 in figure 7) goes to the pipelined triple DES circuit shown in figure 8. FIFO A, 508, and FIFO B, 510, in figure 7 are represented in figure 8 as IN FIFO A, 702 and IN FIFO B, 704, respectively. In order to operate the triple DES circuit at the cell rate, data from the re-formatter circuit 518 is alternately loaded into the two FIFOs 508, 510. The first cell goes into FIFO A, the second cell into FIFO B, the third cell into FIFO A, the fourth cell into FIFO B, etc. The pipelined DES circuit is discussed further in conjunction with figures 10 and 12 below.

PIPELINED TRIPLE DES

The heart of the encryption system is the triple DES processing engine. The chip used in the triple DES processing engine is the VM009B DES Data Ciphering processor from VLSI

Corporation: There are other chips both experimental and commercially available that do encryption. The disadvantage of the VM009B DES chip is that the maximum data rate is a little more than 1/2 the OC-3c cell rate. In order to do triple DES at line rates, a combination of processor pipelining and parallel processing is used. Processor pipelining speeds up a calculation by using multiple processing processors in series. The result from one processing processor is fed into the input of the next processing processor. Parallel processing speeds up calculations by duplicating whole processing pipelines where each processing pipeline works on different data. Used in combination in the present invention, the parallel and serial arrangement of DES chips is determined by the specific process of the encryption engine, the resulting processor pipeline latency and the ATM cell rate. The time to do an encryption process is determined by the processor pipeline latency (i.e., the time between when data enters the first processing engine until the time the results leave the last processing engine). The number of pipelines is determined by the speed of the individual encryption chip. For the OC-3c rate and using triple DES encryption, the individual encryption chip could accept at half the line rate. Therefore, two pipelines were required.

For ECB or Counter Mode encryption at OC-3a rates, the data is partitioned across two banks of devices. To do triple DES encryption, three devices per bank are needed. Each crypto unit requires 12 VM009B DES chips to do bi-directional full speed triple DES, ECB or encryption. For OC-12c data rates, 8 encryption pipelines using three DES chips are required. There are then 8 FIFOs (for 8 parallel pipelined paths), with 3 DES chips (for triple DES) each, times 2 (for bi-directional transfer), for a total of 48 VM009B DES chips.

The encryption delay is one element of system latency. The overall latency is 17 microseconds accounted for as follows:

FUNCTION	NUMBER OF OC-3c CELL TIMES
SONET interface	4
VC lookup	1
DRAM	1
Encryption	2 plus a small "extra" amount
TOTAL	8 cell times or about 17 microseconds

Figure 8 is a block diagram of the triple DES encryption/decryption circuit. The cell data to be encrypted or decrypted is loaded alternately into FIFO A (702) and FIFO B (704). One parallel arm of the triple DES pipeline circuit comprises 3 DES chips, 708, 710, 712 in series, an encryption controller 706, and an output FIFO A (714). A second parallel arm of the triple DES pipeline circuit comprises 3 DES chips, 720, 722, 723 in series, an encryption controller 718, and an output FIFO B (716). The encryption controllers 706, 718 are implemented as state machines. After a complete

cell is stored in one of the input FIFOs 702, 704, the respective encryption controller 706, 718 performs a series of pipeline loads into one or more of the DES chips and/or the output FIFO.

The staggered timing (a processor pipeline) of data and key loads is illustrated in figure 9. The first of the triple DES keys (key 1) is loaded into device A (708 or 720). Thereafter, device A encrypts/decrypts block 1 (later followed by blocks 2 through 6 in succession). While block 1 is being encrypted/decrypted in device A, the second of the triple DES keys (key 2) is loaded in device B. While block 2 is being encrypted/decrypted in device B, the third of the triple DES keys (key 3) is loaded in device C. Then device C (712 or 723) completes the encryption/decryption of block 1. At the end of the pipeline, triple DES encrypted/decrypted data cells are stored in the respective output FIFO (714 or 716).

Prior to the data being available on the output of the third device the crypto system header and ATM header is written into the output FIFO. In order to encrypt/decrypt a cell in the 5.6μs window (two cell times) the encryption circuitry is run with a faster clock than is the rest of the crypto unit circuit. Most of the crypto unit circuitry runs on a 23MHz clock; however, the encryption circuit runs on a 33 MHz clock. There is a gap between block 6 and the next key. That gap is the small amount of "extra" time discussed above. At the above clock rate it takes about 5.55μs for key and data to be processed by the first encryption chip.

Figure 10 is a block diagram overview of the pipelined triple DES encryption/decryption circuit. Alternate cell data is directed to one of two parallel paths, either through one triple DES pipeline 750 or the other parallel triple DES pipeline 752. The encryption/decryption devices operate in serial, as described above. However, all encryption/decryption devices also operate in parallel as well as serial. For example, while the second device is encrypting/decrypting block 1, the first device is encrypting/decrypting block 2. It is the pipelining of chips to do the triple DES functions in combination with a plurality of pipelines that permits the slower DES chips to function in an environment requiring faster triple DES encryption/decryption than any one of the slower DES chips can perform. In figure 9, one cell 1206 is followed by the next cell 1202, and preceded by the previous cell 1204, so that the decryption pipeline is never empty so long as there is data to encrypt/decrypt.

Typically, in performing a triple DES operations, a single chip performs all three DES operations. That is, the output of the chip (the first encryption) is used as the input to the same chip to do the next DES operation (a decryption), and the output of the same chip is used to do the last DES operation (an encryption). In the present invention, a three stage DES pipeline uses three encryptor/decryptors, which concurrently operate on different stages of the encryption/decryption process within the same ATM cell, and on different stages of the encryption/decryption process

between consecutive ATM cells simultaneously.

ALTERNATE EMBODIMENT - COUNTER MODE

Counter Mode for ATM cell encryption is an alternate approach to encryption that uses a method similar to the output feedback mode described in Schneier, B., "Applied Cryptography" second edition, published by John Wiley & Son Inc., New York, NY 1996. Counter Mode is described in the Phase I ATM Security Specification Draft, ATM Forum, BTD-SECURITY-01.03, July 1997, as a proposed encryption standard for ATM. The advantage of Counter Mode over ECB is that it ensures that identical clear text will be encrypted as different cipher text. Counter Mode also has the advantage over CBC in that it can be parallelized such that it will run at a higher data rate than is currently available with CBC. Counter Mode has an advantage over both ECB and CBC in that one bit errors in the received cipher text only cause one bit errors in the clear text. For ECB a 1 bit error causes a 1 block, (i.e., 64 bit) error extension, while for CBC, a 1 bit error causes a 2 block, (i.e., a 128 bit) error extension. The disadvantage of Counter Mode is that cell loss can result in loss of cryptographic synchronization (i.e., all remaining cells are garbled until resynchronized).

Counter Mode works by generating a pseudo random pattern (called a key stream), and combining the clear text and the key stream in an exclusive OR operation. The key stream is generated by starting with a State Vector, and encrypting the State Vector using DES (single or triple) to form the key stream. The encryption/decryption keys are exchanged between the transmitting end and the receiving end as before. At the receiving end, the key stream is independently generated using the encryption keys and State Vector. The clear text is regenerated by combining the received cipher text and the locally generated key stream in an exclusive OR operation.

Figure 6 is a block diagram illustrating Counter Mode. The Counter Mode process steps are:

1.) Generate a non-repeating clear-text pattern called a State Vector,

2.) Encrypt the State Vector (SV) with DES (single or triple) to create the key stream,

3.) Exclusive OR (XOR) the encrypted State Vector with the clear text to produce cipher text,

4.) Transmit the cipher text.

5.) On the receive side, encrypt the same State Vector using the same DES key (single or triple), and

6.) Exclusive OR the received cipher text with the encrypted State Vector (the reconstructed key stream) to recover the clear text.

When an ATM cell to be encrypted arrives, the SV and Key are extracted from the State memory 652. The SV (not the cell) is encrypted using single or triple DES in the encryption circuit 656. The SV is modified for each block using the segment number to ensure that each block has a

different SV number (the cell is 6 DES blocks long). The SV is updated 650 and restored in the DRAM memory 652 so that the new SV will be available for the next ATM cell of the particular VC. The SV, ATM cell, and the encryption keys are sent to one of the encryption pipelines 656 where the SV value is encrypted. The updating of the SV ensures that each cell of a particular VC is combined with a unique SV. The series of SV values, after being encrypted, form a unique pseudo-random number to XOR 658 with the clear text 654. The payload of each cell is exclusive ORed with the encrypted SV to produce the cipher text. For AAL1 and AAL3/4 connections, the first byte is left in the clear. The first byte contains the sequence number which is used as part of the SV. By using the sequence number as part of the SV and allowing the sequence number in the cell to remain clear text, the Counter Mode approach allows for a small number of cells to be dropped for AAL1,3, and 4 connections without losing Counter Mode synchronization. The encrypted cell is then transmitted to the far end, receiving station.

On the receive side, when an encrypted cell arrives, the SV and Key are extracted from the State memory 662. The SV is updated 660 and restored in the State memory 662 so that a new SV will be available for the next cell of the particular VC. The SV, ATM cell, and the encryption. Keys are sent to one of the encryption pipelines 664, where the SV value is then encrypted. Note that for Counter Mode, DES encryption is used both for transmit and receive processes. The encrypted SV forms a unique pseudo-random number to XOR 666 with the received cipher text to reconstruct the clear text output.

COUNTER MODE SYNCHRONIZATION

In order to maintain synchronization, the SV used on the receive side must be the same as that used on the transmit side. The SV contains several fields:

1.) Jump number (35 bits)

2.) Sequence number (4 bits)

3.) Segment number (3 bits)

4.) I/R bit (Initiator/Responder) (1 bit)

5.) Linear feedback shift register (21 bits)

The linear shift register is a 21 bit pseudo random sequence with 2^{21}-1 values. The linear feedback shift register ensures that the SV for each cell is unique. Each time a cell for a VC is received, the SV is modified by changing the linear feedback shift register by one position. For AAL0,2 and 5, the linear feedback shift register is updated one position for every cell. For AAL1,3 and 4, the linear feedback shift register is updated every time the sequence number cycles.

The jump number is used to ensure re-sequencing of SV values in the event of cell loss. In order to ensure synchronization, and to make sure the linear feedback shift register does not cycle

(overflow), the jump number is incremented periodically. The linear feedback shift register resets to a known value when the jump number is incremented. The jump number is incremented when a SESSION KEY CHANGEOVER (SKC) cell is sent from the transmitter to the receiver, and also when the end of message is received for AAL5 packets.

The I/R bit identifies the initiator (the calling party) or responder (the called party). The purpose of the I/R bit is to ensure that a different SV is used for duplex connections which use the same encryption key for transmit and receive.

The sequence number is extracted from the first byte of the ATM cell. For AAL1, the sequence number cycles for 0 to 7; for AAL 3/4 the sequence cycle number cycles for 0 to 15. Since the LFSR is updated only when the sequence number in the ATM cell cycles, the use of the sequence number as part of the SV reduces the likelihood of loss of encryption synchronization in the event of cell loss for AAL1 and AAL3/4 type connections. A connection using AAL1 will require a burst loss of more than 7 cells before encryption sync is lost. AAL3/4 would require a burst loss of more than 15 cells.

Figure 11 is a more detailed embodiment of the block diagram of a pipelined triple DES encryption/decryption engine of figure 8, configured to be used with either ECB or Counter Mode. Two complete pipelines (pipeline A and pipeline B) of triple DES are shown. The pipeline input 1103 is alternately fed to FIFO A, 1102 or FIFO B, 1104 (which are analogous to 702 and 704 in figure 8). Each pipeline comprises an input FIFO 1102, 1104, an encryption controller 1150, 1152, a bypass FIFO 1130, 1140, an output FIFO 1114, 1116, first, second and third DES chips 1108, 1120, 1110, 1122, 1112, 1123. Respective output FIFOs 1114, 1116 (which are analogous to 714 and 716 in figure 8) hold the output of each encryption pipeline. Each encryption controller further contains respective multiplexers 1134 or 1144 to select the appropriate output to respective output FIFOs 1114 or 1116. Since both pipeline A and pipeline B operate in a similar fashion, the operation of pipeline A is described below.

The pipeline input 1103 is either key and State Vector data (for Counter Mode) or ATM cell data (for ECB mode). Three single DES chips 1108, 1110, and 1112 perform triple DES encryption/decryption on either the State Vector (for Counter Mode) or on cell data (for ECB). For single DES operations, the middle DES chip 1110 alone is used. The encryption controller 1150 contains a state machine that will do a series of pipeline loads into one or more of the DES chips 1108, 1110, 1112 and/or the output FIFO 1114 when it has a complete cell in the input FIFO 1102.

In operation, there are three modes: clear text, Counter Mode and ECB mode. For clear text, cell data bypasses the encryption pipeline in FIFO 1130, and is selected by multiplexer 1134 for output to FIFO A, 1114. For ECB mode, cell data is coupled to the input of DES chip 1108 (for

triple DES) or the input of DES chip 1110 (for single DES). For Counter Mode, instead of cell data, key and State Vector data is coupled to the input of DES chip 1108 (triple DES) or to the input of DES chip 1110 (single DES). For Counter Mode, the encrypted SV is XORed 1132 with clear text (for encryption). In the case of decryption, the encrypted SV is XORed 1132 with cipher text. In ECB mode, multiplexer 1134 selects the output DES chip 1112 to go to output FIFO A, 1114. Also for Counter Mode, multiplexer 1134 selects the output of exclusive OR circuit 1132 to go to output FIFO 1114, while for ECB mode, multiplexer 1134 selects the output of DES chip 1112 to go to output FIFO A, 1114. The output of each of the encryption/decryption circuits goes to the SONET transmit circuit where it is multiplexed together into a single stream. The two cipher (or clear) text data streams are multiplexed together by alternating between reading from OUT FIFO A, 1114 and OUT FIFO B, 1116.

In order to encrypt/decrypt a single cell of data (6 DES blocks) in the 5.6 μs window (two cell times) the encryption/decryption circuitry is run faster than the rest of the security system. While most of the security system runs on a 23 MHz clock, the encryption/decryption circuitry is run on a 33 MHz clock. The faster clock provides about 468 ns per cell extra time.

The timing of data through the encryption/decryption pipeline of figure 11 is shown in figure 12. The first key, key 1, is loaded into the first chip before the arrival of Block 1 of clear text. Before the first chip is done encrypting the first block of data, the encryption controller loads the second key, key 2, in the second chip. The encrypted output of the first chip is sent to the input of the second chip. Before the second chip is done with decrypting the first block of data, the encryption controller loads the third key, key 3, into the third chip. The encrypted output of the second chip is fed into the input of the third chip. In vector pipeline, the DES chips are continuously processing data, so long as there are ATM cells to process. The first chip starts encrypting the next block of data from the next ATM cell as soon as it is ready to accept more inputs.

In particular, the timing of an encryption operation through the pipelined triple DES circuit is illustrated in figure 12. The input 1210 to the first DES chip is the first DES key, key 1, followed by the 5 blocks of clear text from the ATM payload, Block 1 through Block 6. The output 1216 of the first DES chip is 5 blocks of singly ciphered text. The second DES key, key 2, is input to the second chip, followed by the output 1218 of the first DES chip. The output 1220 of the second DES chip is 5 blocks of doubly ciphered text. The third DES key, key 3, is input to the third chip, followed by the output 1222 of the second DES chip. The final output 1224 of the third DES chip is 5 blocks of triply ciphered text. The processing of the next cell 1214 begins before the processing of the current input cell 1210 is completed to form the output 1224 of the current cell.

As indicated previously, a single DES chip is capable of performing a sequential triple DES

operation, by using the output of each DES operation as the input to the same chip for the next DES operation. In contrast, in the paralleled pipelined architecture of the present invention, three separate DES encryption/decryption devices are operated in a serial pipeline, with plural serial pipelines in parallel (750, 752 in figure 10). In Figure 12, the encrypted output 1209 corresponding to the previous cell, is followed by the encrypted output 1224 corresponding to the current cell 1210, which is followed by the encrypted output (not shown) corresponding to the next cell 1214. Although the triple DES process for 1 ATM cell requires 2 ATM cell times, or about 5.6 μs, the use of two pipelines in parallel brings the average processing time to within the time frame of a single ATM cell.

HOST INTERFACE

The host interface consists of an 8 bit SBUS slave interface. When the host performs a 32 bit word access, the host interface breaks up the access into four 8-bit accesses before issuing an acknowledgment. While this slows down SBUS slave cycles slightly, it saves considerably in the size of data movement and the amount of hardware necessary for host access. An 8-bit internal interface and SBUS slave interface is adequate for the amount of data movement across the bus, i.e., for updating internal tables and registers and for reading and writing the data FIFO.

The highest bandwidth demands are for the extraction and insertion FIFOs. The maximum data transfer rate between the extraction FIFO and the host is expected to be no more than 100K bits per second (assuming 100 connection attempts per second and Q.2931 messages). The maximum (realizable) data rate is about 4 MBytes/second using slave mode access. Therefore, there is plenty of bandwidth for data movement, without using a faster bus or DVMA access.

One memory location that needs special attention is the state memory associated with the encryption/decryption. This memory is a single port DRAM memory where access is scheduled. Reads and writes to this memory must occur only at certain times. The access mechanism is by means of a buffer register. To write into memory, the host writes the address and data to the buffer register. Then, during the scheduled times that host accesses are allowed, the data is written into the DRAM. Consecutive writes need to be separated by about 2μs. For reads from this memory, the host performs two reads, the first is a dummy read where the address to be read is loaded into the buffer register, and then followed (about 1μs later) by a second read. Once the scheduled host access time occurs for a read, the content of the memory location is loaded into the buffer register. On the second read, the content of the register is returned to the host.

What is Claimed Is:

1. In an ATM communication system for transmitting and receiving data formatted into ATM cells, each ATM cell including a header portion and a payload portion therein, first and second host systems being coupled to said ATM communication system and connected to each other through said ATM communication system, first and second cryptographic units disposed as an interface between said ATM communication system and first and second host systems respectively, each said first and second cryptographic units encrypting or decrypting at least a portion of said ATM cell, each said first and second cryptographic units having cryptographic state information values associated therewith representing the cryptographic state of said first and second cryptographic units, said header portion of said ATM cell including a virtual circuit number representing a virtual circuit between said first and second host systems connected to each other through said first and second cryptographic units, a method for determining the cryptographic state information values for a given cryptographic state corresponding to a received virtual circuit number, said method comprising:

storing a plurality of said cryptographic state information values for a plurality of cryptographic states respectively corresponding to a plurality of active virtual circuit numbers;

arranging said plurality of active virtual circuit numbers in substantially numerical order to form an ordered list of virtual circuit numbers;

storing said ordered list of virtual circuit numbers in a lookup table, said lookup table providing a link between each of said plurality of active virtual circuit numbers and a corresponding one of said plurality of said cryptographic state information values;

receiving an ATM cell containing an ATM header portion;

receiving a virtual circuit number contained in said ATM header portion to form said received virtual circuit number;

comparing said received virtual circuit number to individual ones of said plurality of virtual circuit numbers stored in said lookup table to find a match between said received virtual circuit number and a given one of said plurality of said active virtual circuit numbers stored in said lookup table; and

retrieving said cryptographic state information values for said given cryptographic state corresponding to said received virtual circuit number.

2. A method in accordance with claim 1, wherein said step of arranging said plurality of active virtual circuit numbers in substantially numerical order to form an ordered list of virtual circuit numbers comprises arranging said plurality of active virtual circuit numbers in substantially ascending numerical order in substantially ascending memory address locations.

3. A method in accordance with claim 1, wherein said step of comparing said received virtual circuit

number to individual ones of said plurality of virtual circuit numbers stored in said lookup table to find a match between said received virtual circuit number and a given one of said plurality of said active virtual circuit numbers stored in said lookup table, further comprises:

accessing said stored lookup table at a first memory address location to form a first accessed table address;

comparing the virtual circuit number from the contents of said first accessed table address to said received virtual circuit number;

accessing said stored lookup table at a second memory address location, greater than said first memory address location, if said virtual circuit number from the contents of said first accessed table address is greater than said received virtual circuit number; and

accessing said stored lookup table at a third memory address location, less than said first memory address location, if said virtual circuit number from the contents of said first accessed table address is less than said received virtual circuit number.

4. A method in accordance with claim 3, wherein said method is a binary search method, said first memory address location being substantially corresponding to the one half point of said lookup table, said second memory address location substantially corresponding to the one quarter point of said lookup table and said third memory address location substantially corresponding to the three fourths point of said lookup table.

5. A method in accordance with claim 1, further including the step of applying said retrieved cryptographic state information values to condition said first cryptographic unit to encrypt a clear text ATM payload.

6. A method in accordance with claim 1, further including the step of applying said retrieved cryptographic state information values to condition said second cryptographic unit to decrypt a cipher text ATM payload.

7. A method in accordance with claim 1, further including the step of storing a plurality of index vectors in said lookup table, each of said index vectors corresponding to said plurality of active virtual circuits.

8. A method in accordance with claim 7, wherein said step of retrieving said cryptographic state information values for said given cryptographic state corresponding to said received virtual circuit number includes using said index vector as a memory address pointer to one of said plurality of said cryptographic state information values.

9. A method in accordance with claim 1, wherein said method further comprises:

storing an additional one of said cryptographic state information values for an additional one of said plurality of cryptographic states corresponding to an additional active virtual circuit number;

arranging said plurality of active virtual circuit numbers including said additional active circuit number, in substantially numerical order to form a second ordered list of virtual circuit numbers;

storing said second ordered list of virtual circuit numbers in a second lookup table, said second lookup table providing a link between each of said plurality of active virtual circuit numbers plus said additional virtual circuit number and a corresponding one of said plurality of said cryptographic state information values including said additional one of said cryptographic state information values; and

substituting said second ordered list in said second lookup table for said ordered list in said lookup table.

10. In an ATM communication system for transmitting and receiving data formatted into ATM cells, each ATM cell including a header portion and a payload portion therein, first and second host systems being coupled to said ATM communication system and connected to each other through said ATM communication system, first and second cryptographic units disposed as an interface between said ATM communication system and first and second host systems respectively, each said first and second cryptographic units encrypting or decrypting at least a portion of said ATM cell, each said first and second cryptographic units having cryptographic state information values associated therewith representing the cryptographic state of said first and second cryptographic units, said header portion of said ATM cell including a virtual circuit number representing a virtual circuit between said first and second host systems connected to each other through said first and second cryptographic units, an apparatus for determining the cryptographic state information values for a given cryptographic state corresponding to a received virtual circuit number, said apparatus comprising:

storing a plurality of said cryptographic state information values for a plurality of cryptographic states respectively corresponding to a plurality of active virtual circuit numbers;

arranging said plurality of active virtual circuit numbers in substantially numerical order to form an ordered list of virtual circuit numbers;

storing said ordered list of virtual circuit numbers in a lookup table, said lookup table providing a link between each of said plurality of active virtual circuit numbers and a corresponding one of said plurality of said cryptographic state information values;

receiving an ATM cell containing an ATM header portion;

receiving a virtual circuit number contained in said ATM header portion to form said received virtual circuit number;

comparing said received virtual circuit number to individual ones of said plurality of virtual

of virtual circuit numbers stored in said lookup table to have match between circuit numbers stored in said lookup table to find a match between said received virtual circuit number and a given one of said plurality of said active virtual circuit numbers stored in said lookup table; and

retrieving said cryptographic state information values for said given cryptographic state corresponding to said received virtual circuit number.

11. An apparatus in accordance with claim 10, wherein said means for arranging said plurality of active virtual circuit numbers in substantially numerical order to form an ordered list of virtual circuit numbers comprises arranging said plurality of active virtual circuit numbers in substantially ascending numerical order in substantially ascending memory address locations.

12. An apparatus in accordance with claim 11, wherein said means for comparing said received virtual circuit number to individual ones of said plurality of virtual circuit numbers stored in said lookup table to find a match between said received virtual circuit number and a given one of said plurality of said active virtual circuit numbers stored in said lookup table, further comprises:

accessing said stored lookup table at a first memory address location to form a first accessed table address;

comparing the virtual circuit number from the contents of said first accessed table address to said received virtual circuit number;

accessing said stored lookup table at a second memory address location, greater than said first memory address location, if said virtual circuit number from the contents of said first accessed table address is greater than said received virtual circuit number; and

accessing said stored lookup table at a third memory address location, less than said first memory address location, if said virtual circuit number from the contents of said first accessed table address is less than said received virtual circuit number.

13. An apparatus in accordance with claim 12, wherein said apparatus is a binary search apparatus, said first memory address location being substantially corresponding to the one half point of said lookup table, said second memory address location substantially corresponding to the one quarter point of said lookup table and said third memory address location substantially corresponding to the three fourths point of said lookup table.

14. An apparatus in accordance with claim 10, further including the means for applying said retrieved cryptographic state information values to condition said first cryptographic unit to encrypt a clear text ATM payload.

15. An apparatus in accordance with claim 10, further including the means for applying said retrieved cryptographic state information values to condition said second cryptographic unit to decrypt a cipher text ATM payload.

16. An apparatus in accordance with claim 10, further including the means for storing a plurality of index vectors in said lookup table, each of said index vectors corresponding to said plurality of active virtual circuits.

17. An apparatus in accordance with claim 16, wherein said means for retrieving said cryptographic state information values for said given cryptographic state corresponding to said received virtual circuit number includes using said index vector as a memory address pointer to one of said plurality of said cryptographic state information values.

18. An apparatus in accordance with claim 10, wherein said apparatus further comprises:

means for storing an additional one of said cryptographic state information values for an additional one of said plurality of cryptographic states corresponding to an additional active virtual circuit number;

means for arranging said plurality of active virtual circuit numbers including said additional active circuit number, in substantially numerical order to form a second ordered list of virtual circuit numbers;

means for storing said second ordered list of virtual circuit numbers in a second lookup table, said second lookup table providing a link between each of said plurality of active virtual circuit numbers plus said additional virtual circuit number and a corresponding one of said plurality of said cryptographic state information values including said additional one of said cryptographic state information values; and

means for substituting said second ordered list in said second lookup table for said ordered list in said lookup table.

19. In an ATM communication system for transmitting and receiving data formatted into ATM cells, each ATM cell including a header portion and a payload portion therein, first and second host systems being coupled to said ATM communication system and connected to each other through said ATM communication system, first and second cryptographic units disposed as an interface between said ATM communication system and first and second host systems respectively, each said first and second cryptographic units encrypting or decrypting at least a portion of said ATM cell, an encryption/decryption apparatus having an input data terminal for receiving input data corresponding to said payload portion, and an output data terminal for providing output data corresponding to an encryption or decryption of said payload portion, said encryption/decryption apparatus comprising:

first, second, third and fourth memory circuits, each having respective input and output terminals;

first and second encryption/decryption circuits, each having respective input and output terminals;

said input terminal of said first memory and said input terminal of said second memory being coupled to said input data terminal;

said output terminal of said first memory circuit being coupled to the input terminal of said first said encryption/decryption circuit;

said output terminal of said second memory circuit being coupled to the input terminal of said second encryption/decryption circuit;

said output terminal of said first encryption/decryption circuit being coupled to the input terminal of said third memory;

said output terminal of said second encryption/decryption circuit being coupled to the input terminal of said fourth memory; and

said output terminal of said third memory and said output terminal of said fourth memory being coupled to said output data terminal.

20. An apparatus in accordance with claim 19, wherein said first, second, third and fourth memory circuits each comprise a FIFO circuit.

21. An apparatus in accordance with claim 19, wherein said first and second encryption/decryption circuits each comprise a triple DES encryption/decryption circuit.

22. An apparatus in accordance with claim 19, wherein said encryption/decryption circuit is an encryption circuit comprising:

first, second and third DES circuits, having respective input and output terminals;

the output terminal of said first DES circuit being coupled to the input terminal of said second DES circuit; and

the output terminal of said second DES circuit being coupled to the input terminal of said third DES circuit; wherein,

said first and third DES circuits are configured to perform DES encryption, and said second DES circuit is configured to perform decryption.

23. An apparatus in accordance with claim 19, wherein said encryption/decryption circuit is a decryption circuit comprising:

first, second and third DES circuits, having respective input and output terminals;

the output terminal of said first DES circuit being coupled to the input terminal of said second DES circuit; and

the output terminal of said second DES circuit being coupled to the input terminal of said third DES circuit; wherein,

said first and third DES circuits are configured to perform DES decryption, and said second DES circuit is configured to perform encryption.

24. In an ATM communication system for transmitting and receiving data formatted into a plurality of serial ATM cells, including at least a first ATM cell followed by a second ATM cell, each said first and second ATM cells including a respective first and second header portion and a respective first and second encrypted payload portion therein, a method for decrypting said first and second encrypted payload portions, said method comprising:

receiving said first encrypted payload;

coupling said first encrypted payload to a first decryption circuit;

beginning decryption of said first encrypted payload in said first decryption circuit;

receiving said second encrypted payload during decryption of said first encrypted payload in said first decryption circuit;

coupling said second encrypted payload to a second decryption circuit;

completing decryption of said first encrypted payload in said first decryption circuit to form a first decrypted payload; and

completing decryption of said second encrypted payload in said second decryption circuit to form a second decrypted payload; wherein

said step of beginning decryption of said second encrypted payload in said second decryption circuit is subsequent to said step of beginning decryption of said first encrypted payload in said first decryption circuit, and before said step of completing decryption of said first encrypted payload in said first decryption circuit.

25. A method in accordance claim 24, wherein said steps of receiving said first and second encrypted payloads further includes the steps of:

storing said first encrypted payload in a first memory; and

storing said second encrypted payload in a second memory.

26. A method in accordance with claim 24, further including the steps of:

storing said first decrypted payload in a third memory;

transmitting said first decrypted payload from said third memory;

storing said second decrypted payload in a fourth memory; and

transmitting said second decrypted payload from said fourth memory after said step of transmitting said first decrypted payload from said third memory to form a multiplexed data stream of first and second decrypted payloads.

27. In an ATM communication system for transmitting and receiving data formatted into a plurality of serial ATM cells, including at least a first ATM cell followed by a second ATM cell, each said first and second ATM cells including a respective first and second header portion and a respective first and second clear text payload portion therein, a method for encrypting said first and second

clear text payloads, said method comprising:

receiving said first clear text payload;

coupling said first clear text payload to a first encryption circuit;

beginning encryption of said first clear text payload in said first encryption circuit;

receiving said second clear text payload during encryption of said first clear text payload in said first encryption circuit;

coupling said second clear text payload to said second encryption circuit;

completing encryption of said first clear text payload in said first encryption circuit to form a first encrypted payload; and

completing encryption of said second clear text payload in said second encryption circuit to form a second encrypted payload; wherein

said step of beginning encryption of said second clear text payload in said second encryption circuit is subsequent to said step of beginning encryption of said first clear text payload in said first encryption circuit, and before said step of completing encryption of said first clear text payload in said first encryption circuit.

28. A method in accordance claim 27, wherein said steps of receiving said first and second clear text payloads further includes the steps of:

storing said first clear text payload in a first memory; and

storing said second clear text payload in a second memory.

29. A method in accordance with claim 27, further including the steps of:

storing said first encrypted payload in a third memory;

transmitting said first encrypted payload from said third memory;

storing said second encrypted payload in a fourth memory; and

transmitting said second encrypted payload from said fourth memory after said step of transmitting said first encrypted payload from said third memory to form a multiplexed data stream of first and second encrypted payloads.

30. In an ATM communication system for transmitting and receiving data formatted into ATM cells, each ATM cell including a header portion and a payload portion therein,

first and second host systems being coupled to said ATM communication system and connected to each other through said ATM communication system, first and second cryptographic units disposed as an interface between said ATM communication system and first and second host systems respectively, each said first and second cryptographic units encrypting at least a portion of said ATM cell, each said first and second cryptographic units having cryptographic state information values associated therewith representing the cryptographic state of said first and second

cryptographic units, said header portion of said ATM cell including a virtual circuit number representing a virtual circuit between said first and second host systems connected to each other through said first and second cryptographic units, a method for encrypting said payload portion, said method comprising:

storing a plurality of said cryptographic state information values for a plurality of cryptographic states respectively corresponding to a plurality of active virtual circuit numbers;

arranging said plurality of active virtual circuit numbers to form a list of virtual circuit numbers;

storing said list of virtual circuit numbers in a lookup table, said lookup table providing a link between each of said plurality of active virtual circuit numbers and a corresponding one of said plurality of said cryptographic state information values;

receiving an ATM cell containing a received ATM header portion and a received ATM payload portion;

receiving a virtual circuit number contained in said received ATM header portion to form a received virtual circuit number;

comparing said received virtual circuit number to individual ones of said plurality of virtual circuit numbers stored in said lookup table to find a match between said received virtual circuit number and a given one of said plurality of said active virtual circuit numbers stored in said lookup table;

retrieving said cryptographic state information values for said given cryptographic state corresponding to said received virtual circuit number;

conditioning an encryption process to said given cryptographic state corresponding to said received virtual circuit number; and

encrypting said received ATM payload by said encryption process.

31. A method in accordance with claim 30, wherein said encryption process is a single DES encryption process.

32. A method in accordance with claim 30, wherein said encryption process is a triple DES encryption process.

33. In an ATM communication system for transmitting and receiving data formatted into ATM cells, each ATM cell including a header portion and a payload portion therein,

first and second host systems being coupled to said ATM communication system and connected to each other through said ATM communication system, first and second cryptographic units disposed as an interface between said ATM communication system and first and second host systems respectively, each said first and second cryptographic units decrypting at least a portion of

said ATM cell; each said first and second cryptographic units having cryptographic state information values associated therewith representing the cryptographic state of said first and second cryptographic units, said header portion of said ATM cell including a virtual circuit number representing a virtual circuit between said first and second host systems connected to each other through said first and second cryptographic units, a method for decrypting said payload portion, said method comprising:

storing a plurality of said cryptographic state information values for a plurality of cryptographic states respectively corresponding to a plurality of active virtual circuit numbers;

arranging said plurality of active virtual circuit numbers to form a list of virtual circuit numbers;

storing said list of virtual circuit numbers in a lookup table, said lookup table providing a link between each of said plurality of active virtual circuit numbers and a corresponding one of said plurality of said cryptographic state information values;

receiving an ATM cell containing a received ATM header portion and a received ATM payload portion;

receiving a virtual circuit number contained in said received ATM header portion to form a received virtual circuit number;

comparing said received virtual circuit number to individual ones of said plurality of virtual circuit numbers stored in said lookup table to find a match between said received virtual circuit number and a given one of said plurality of said active virtual circuit numbers stored in said lookup table;

retrieving said cryptographic state information values for said given cryptographic state corresponding to said received virtual circuit number;

conditioning a decryption process to said given cryptographic state corresponding to said received virtual circuit number; and

decrypting said received ATM payload by said decryption process.

34. A method in accordance with claim 33, wherein said decryption process is a single DES decryption process.

35. A method in accordance with claim 33, wherein said decryption process is a triple DES decryption process.

36. In an ATM communication system for transmitting and receiving data formatted into ATM cells, each ATM cell including a header portion and a payload portion therein, first and second host systems being coupled to said ATM communication system and connected to each other through said ATM communication system, first and second cryptographic units disposed as an interface between

said ATM communication system and first and second host systems respectively, each said first and second cryptographic units encrypting at least a portion of said ATM cell, each said first and second cryptographic units having cryptographic state information values associated therewith representing the cryptographic state of said first and second cryptographic units, said header portion of said ATM cell including a virtual circuit number representing a virtual circuit between said first and second host systems connected to each other through said first and second cryptographic units, an apparatus for encrypting said payload portion, said apparatus comprising:

means for storing a plurality of said cryptographic state information values for a plurality of cryptographic states respectively corresponding to a plurality of active virtual circuit numbers;

means for arranging said plurality of active virtual circuit numbers to form a list of virtual circuit numbers;

means for storing said list of virtual circuit numbers in a lookup table, said lookup table providing a link between each of said plurality of active virtual circuit numbers and a corresponding one of said plurality of said cryptographic state information values;

means for receiving an ATM cell containing a received ATM header portion and a received ATM payload portion;

means for receiving a virtual circuit number contained in said received ATM header portion to form a received virtual circuit number;

means for comparing said received virtual circuit number to individual ones of said plurality of virtual circuit numbers stored in said lookup table to find a match between said received virtual circuit number and a given one of said plurality of said active virtual circuit numbers stored in said lookup table;

means for retrieving said cryptographic state information values for said given cryptographic state corresponding to said received virtual circuit number;

means for conditioning a encryption circuit to said given cryptographic state corresponding to said received virtual circuit number; and

means for encrypting said received ATM payload by said encryption circuit.

37. An apparatus in accordance with claim 36, wherein said encryption circuit is a single DES encryption circuit.

38. An apparatus in accordance with claim 36, wherein said encryption circuit is a triple DES encryption circuit.

39. In an ATM communication system for transmitting and receiving data formatted into ATM cells, each ATM cell including a header portion and a payload portion therein, first and second host systems being coupled to said ATM communication system and connected to each other through said

ATM communication system, first and second cryptographic units disposed as an interface between said ATM communication system and first and second host systems respectively, each said first and second cryptographic units decrypting at least a portion of said ATM cell, each said first and second cryptographic units having cryptographic state information values associated therewith representing the cryptographic state of said first and second cryptographic units, said header portion of said ATM cell including a virtual circuit number representing a virtual circuit between said first and second host systems connected to each other through said first and second cryptographic units, an apparatus for decrypting said payload portion, said apparatus comprising:

means for storing a plurality of said cryptographic state information values for a plurality of cryptographic states respectively corresponding to a plurality of active virtual circuit numbers;

means for arranging said plurality of active virtual circuit numbers to form a list of virtual circuit numbers;

means for storing said list of virtual circuit numbers in a lookup table, said lookup table providing a link between each of said plurality of active virtual circuit numbers and a corresponding one of said plurality of said cryptographic state information values;

means for receiving an ATM cell containing a received ATM header portion and a received ATM payload portion;

means for receiving a virtual circuit number contained in said received ATM header portion to form a received virtual circuit number;

means for comparing said received virtual circuit number to individual ones of said plurality of virtual circuit numbers stored in said lookup table to find a match between said received virtual circuit number and a given one of said plurality of said active virtual circuit numbers stored in said lookup table;

means for retrieving said cryptographic state information values for said given cryptographic state corresponding to said received virtual circuit number;

means for conditioning a decryption circuit to said given cryptographic state corresponding to said received virtual circuit number; and

means for decrypting said received ATM payload by said decryption circuit.

40. An apparatus in accordance with claim 39, wherein said decryption circuit is a single DES decryption circuit.

41. An apparatus in accordance with claim 39, wherein said decryption circuit is a triple DES decryption circuit.

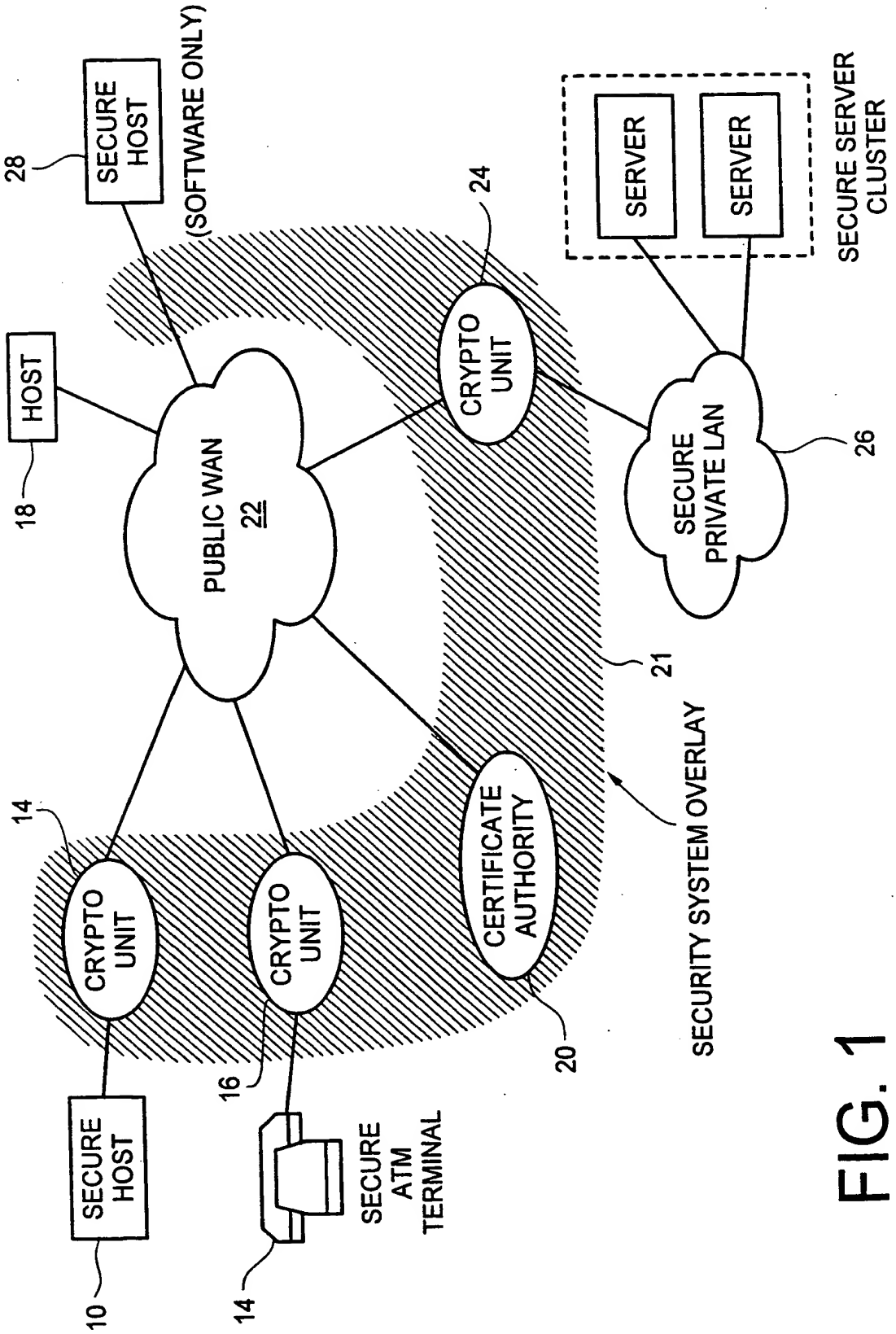


FIG. 1

FIG. 2

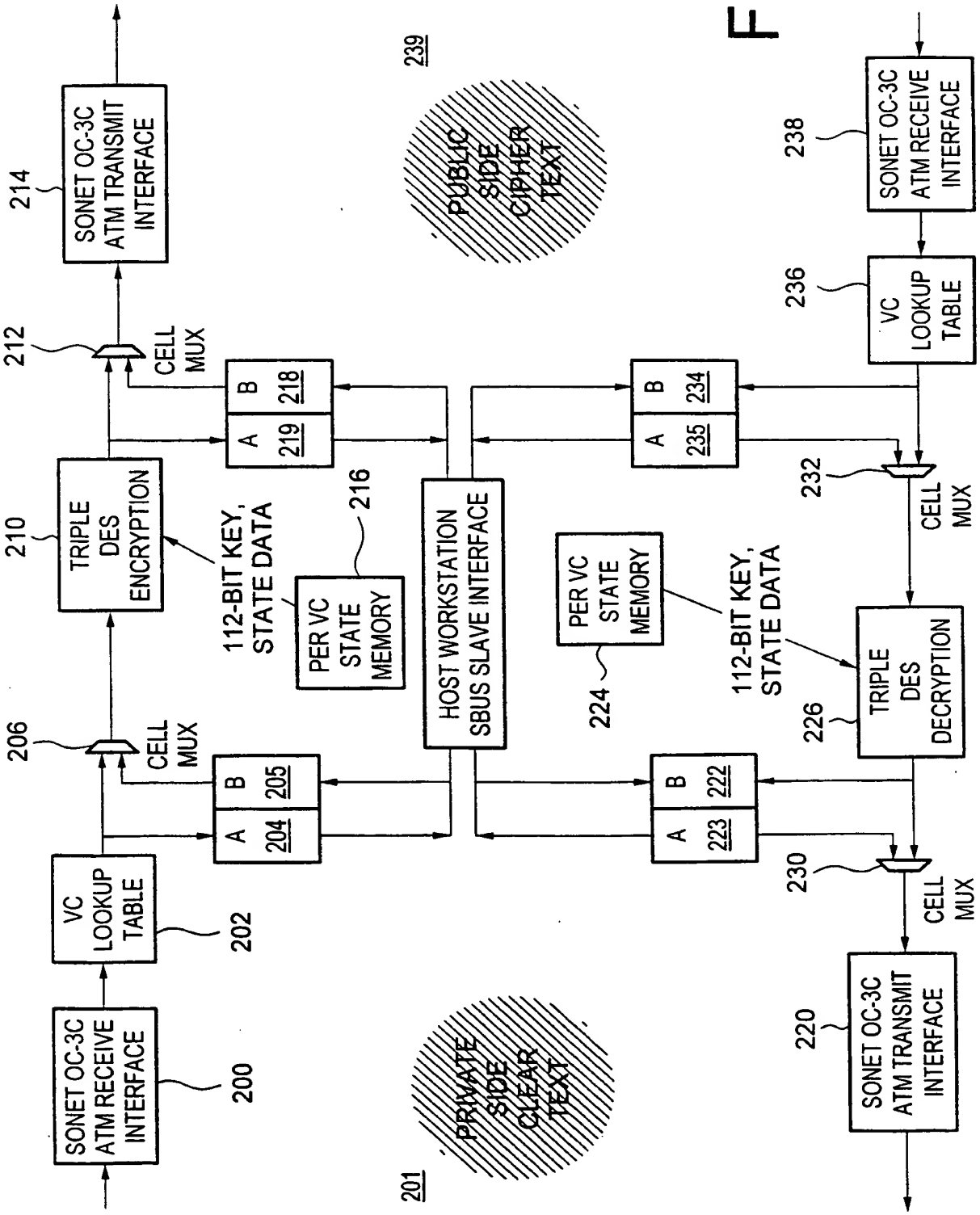
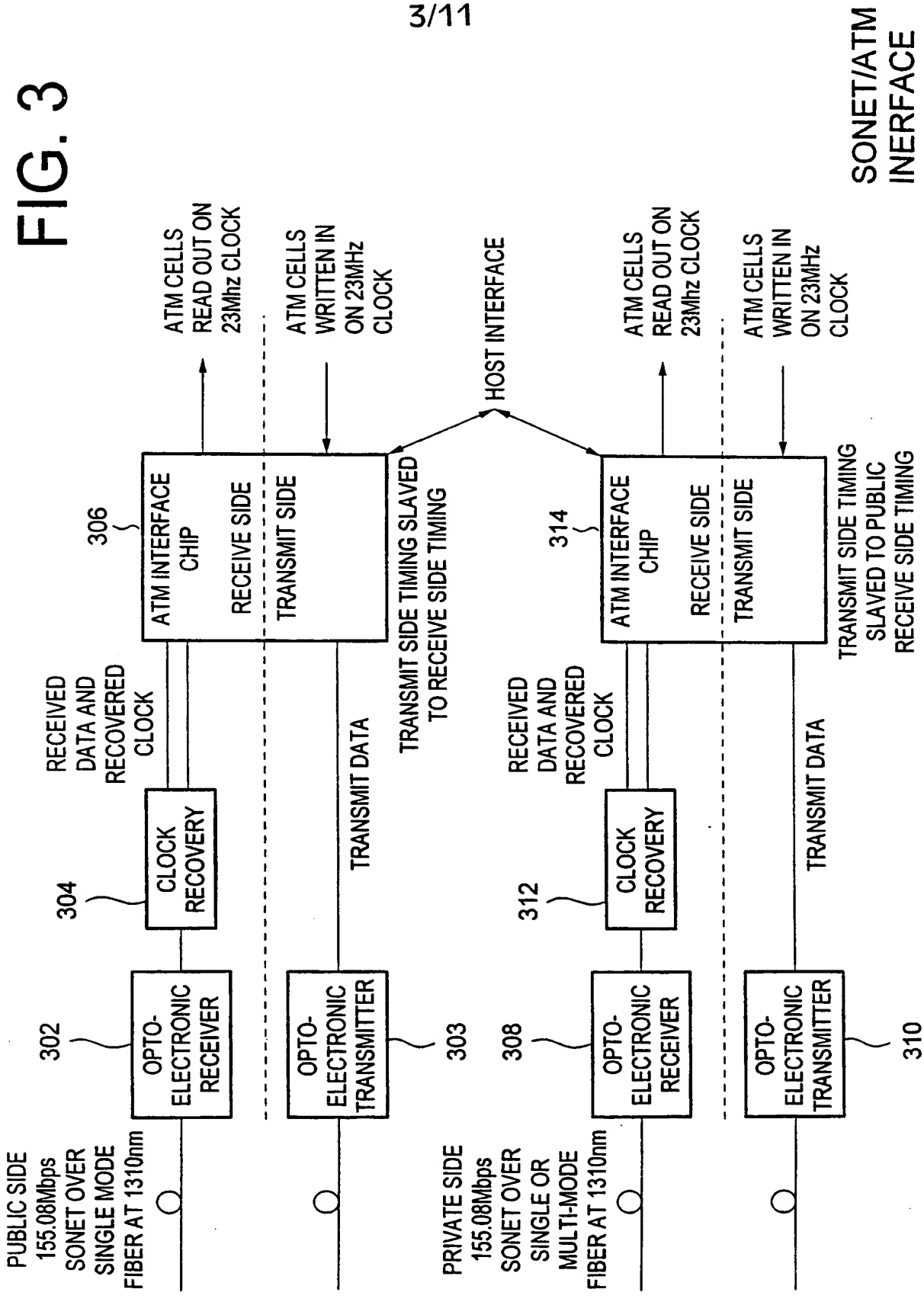


FIG. 3



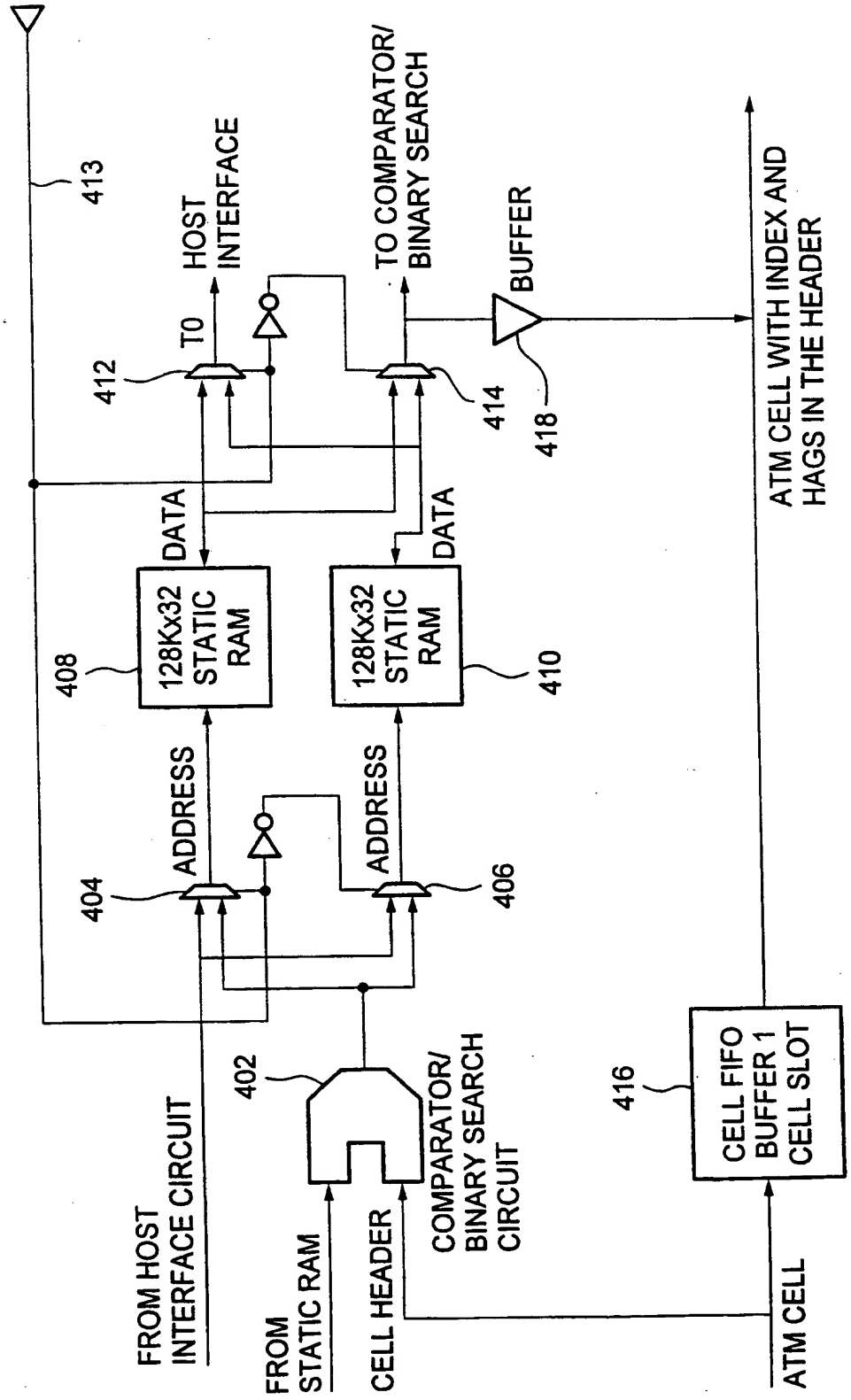
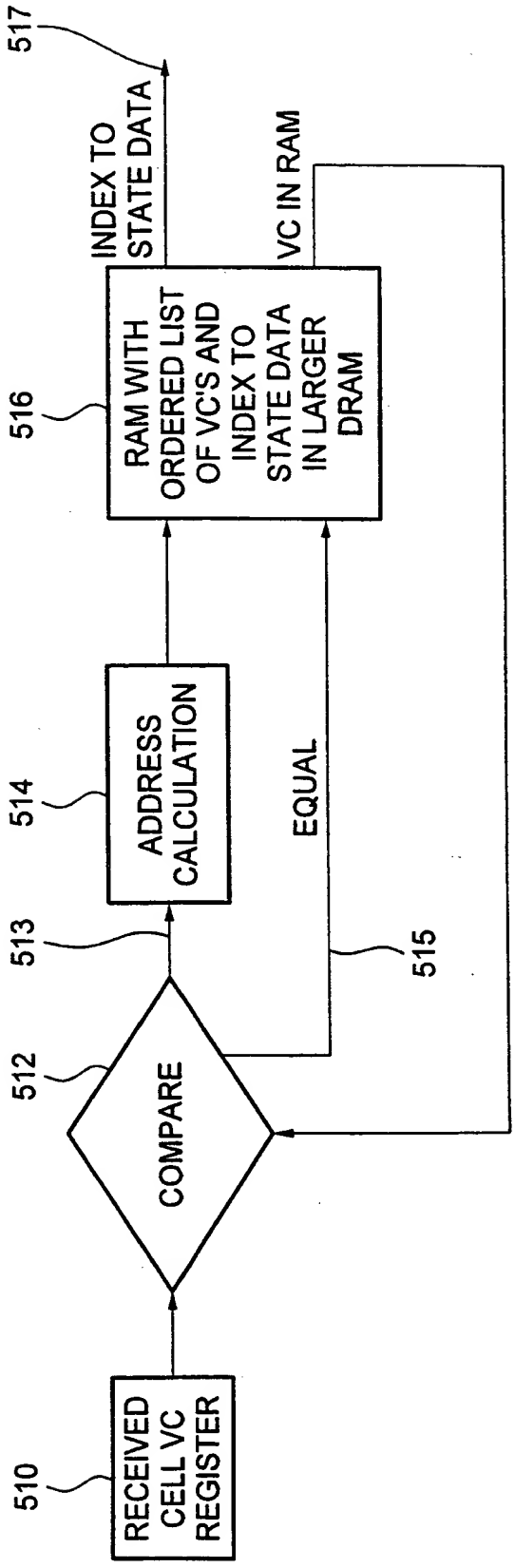


FIG. 4



VC LOOKUP

FIG. 5

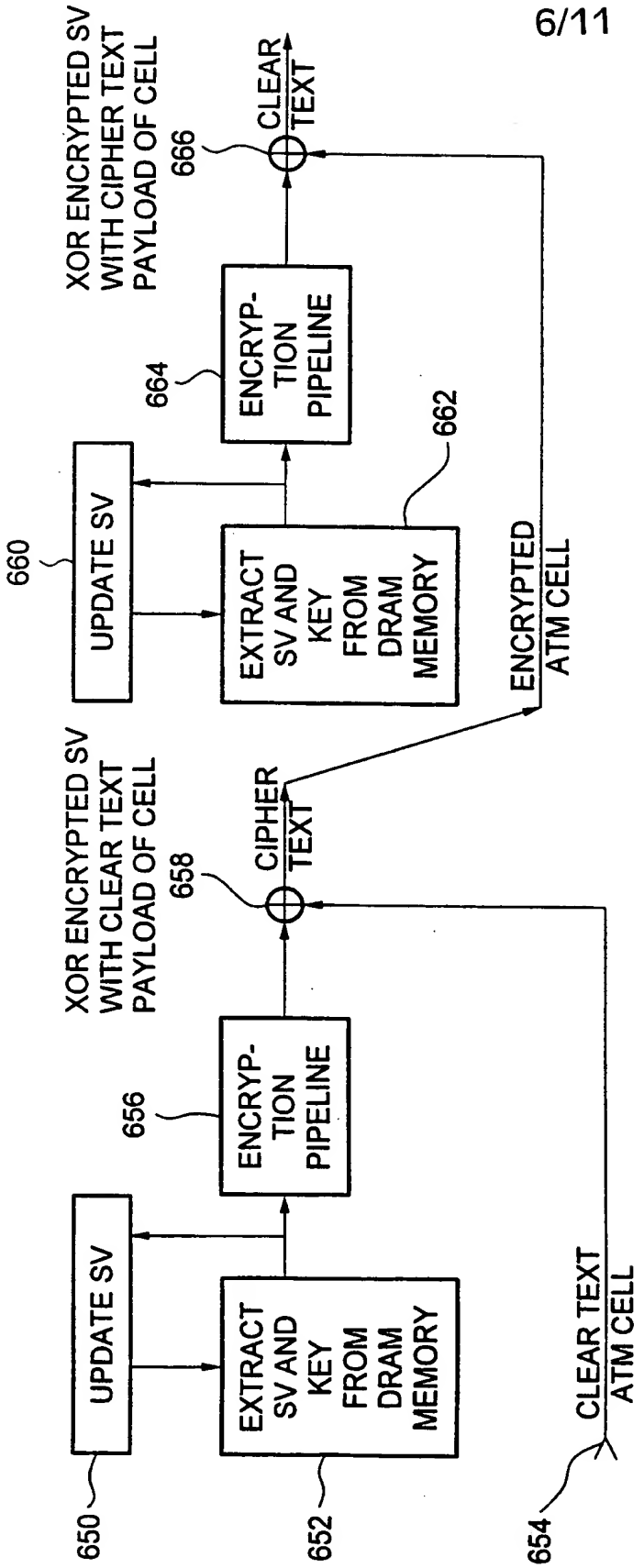


FIG. 6

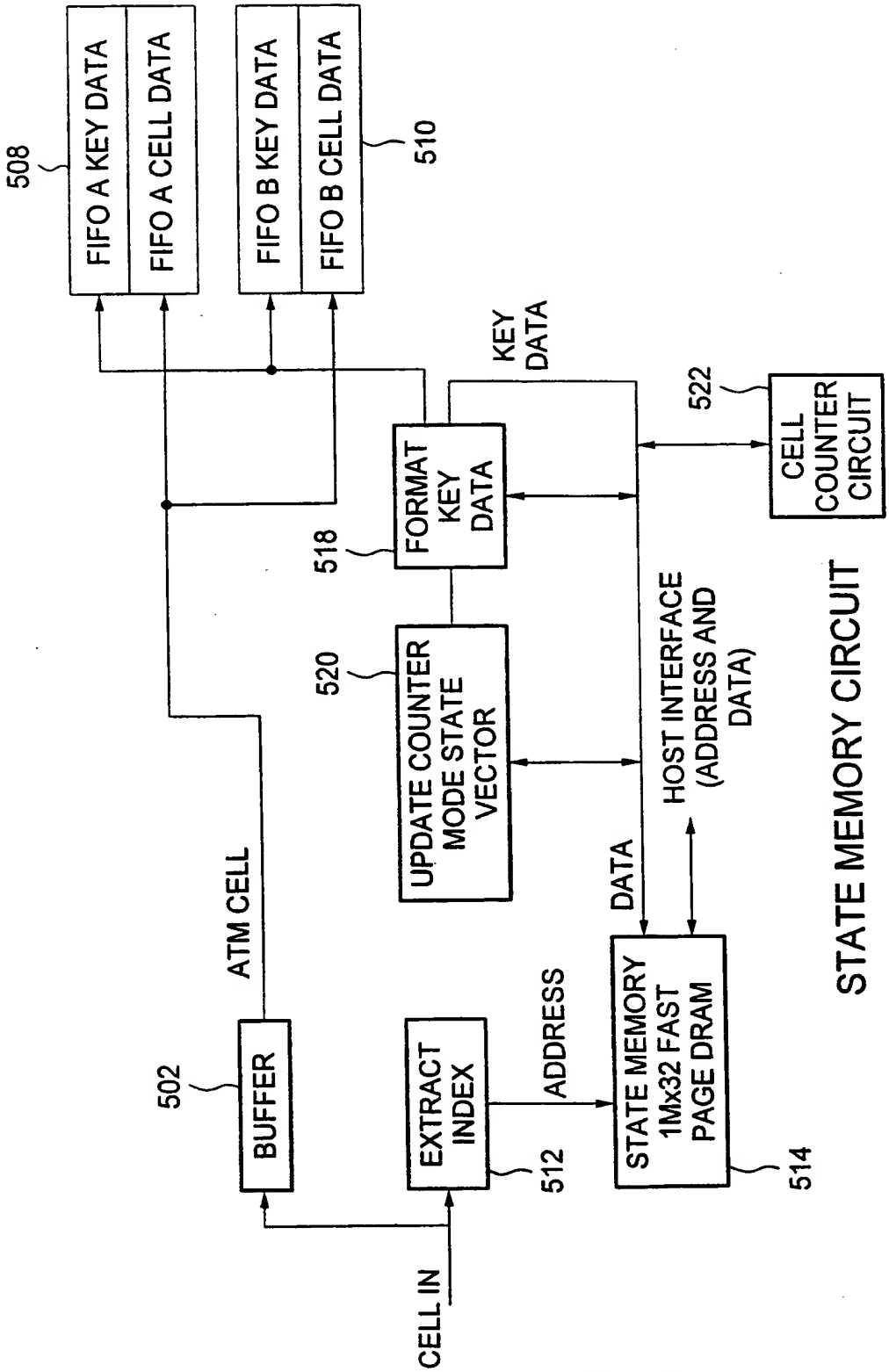
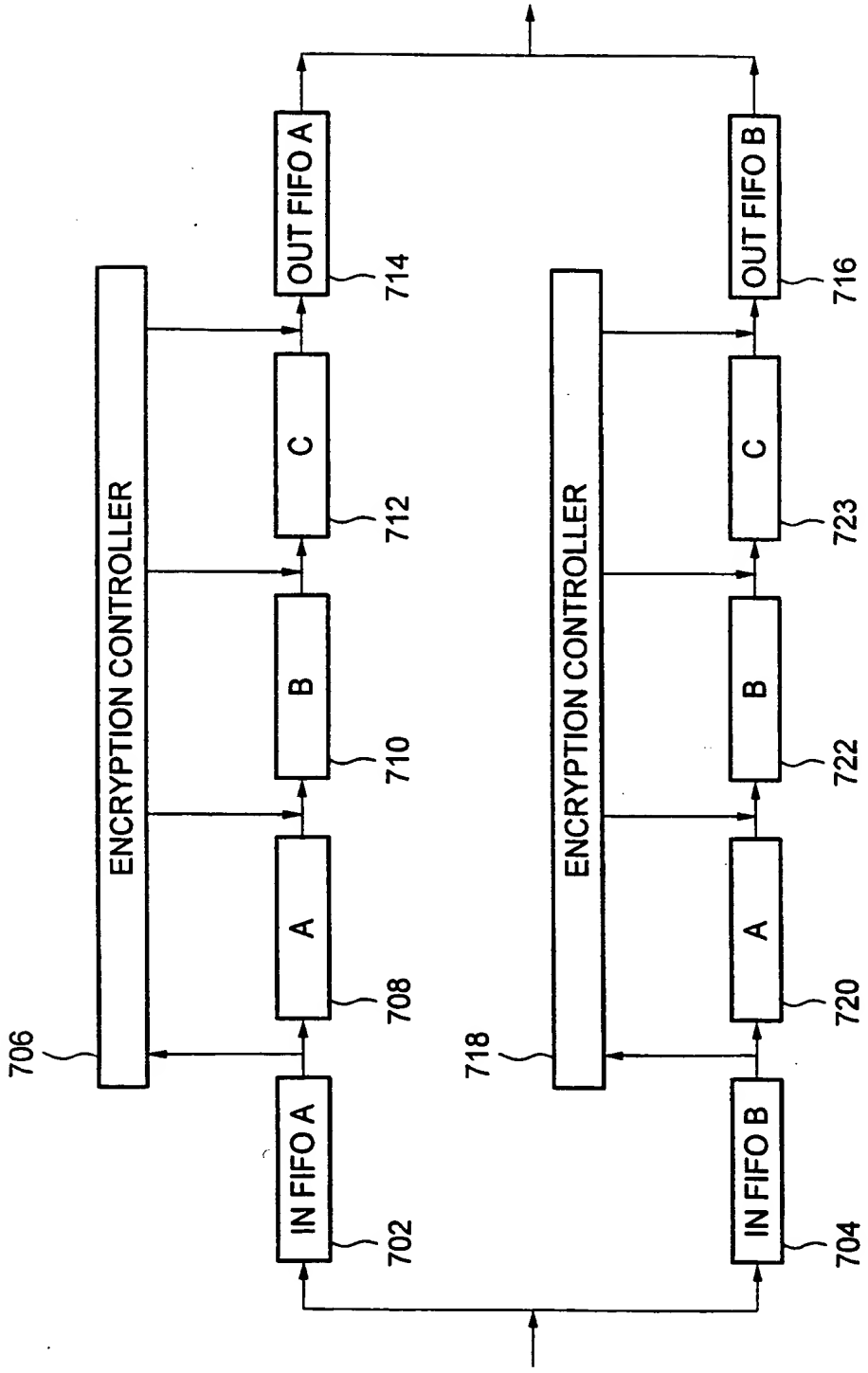


FIG. 7



TRIPLE DES ENCRYPTION

FIG. 8

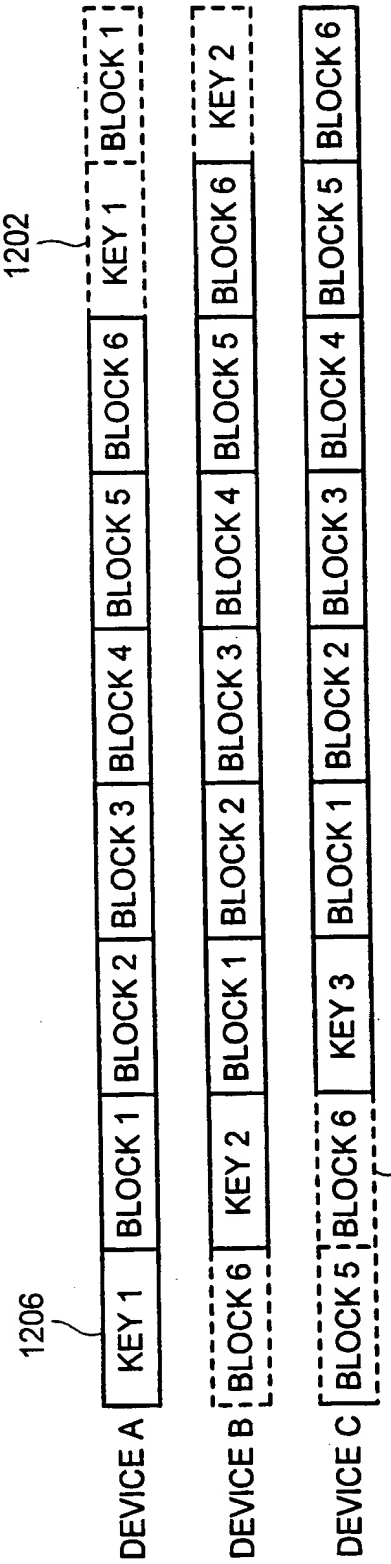


FIG. 9

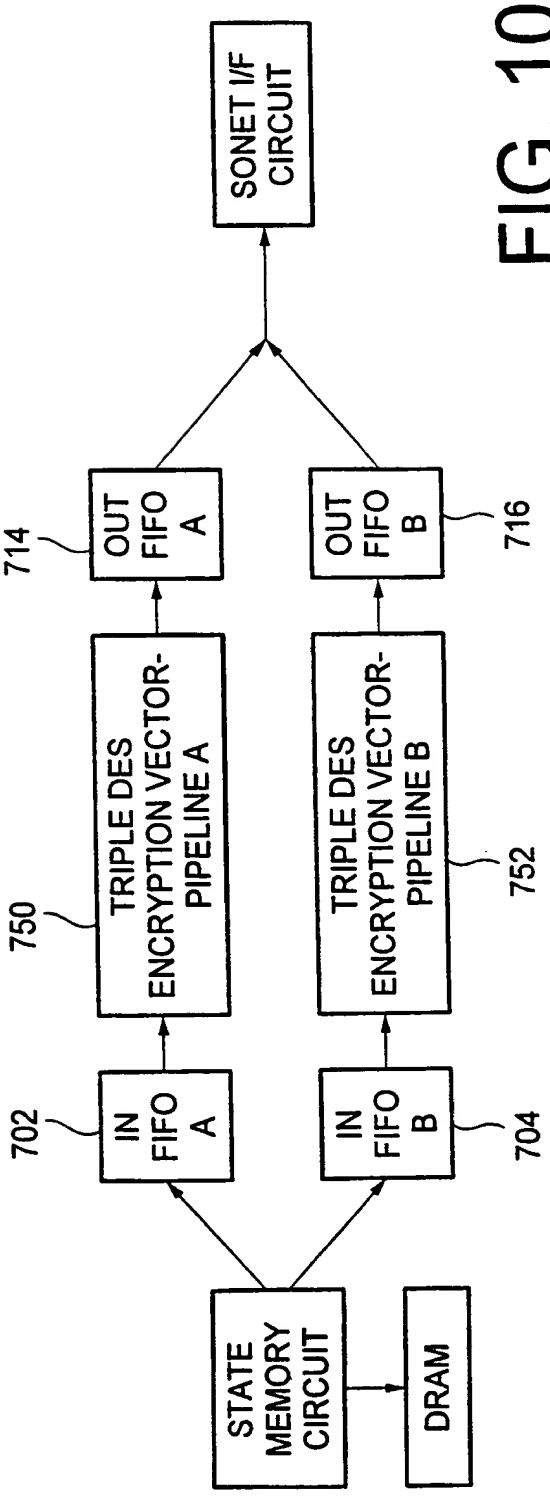


FIG. 10

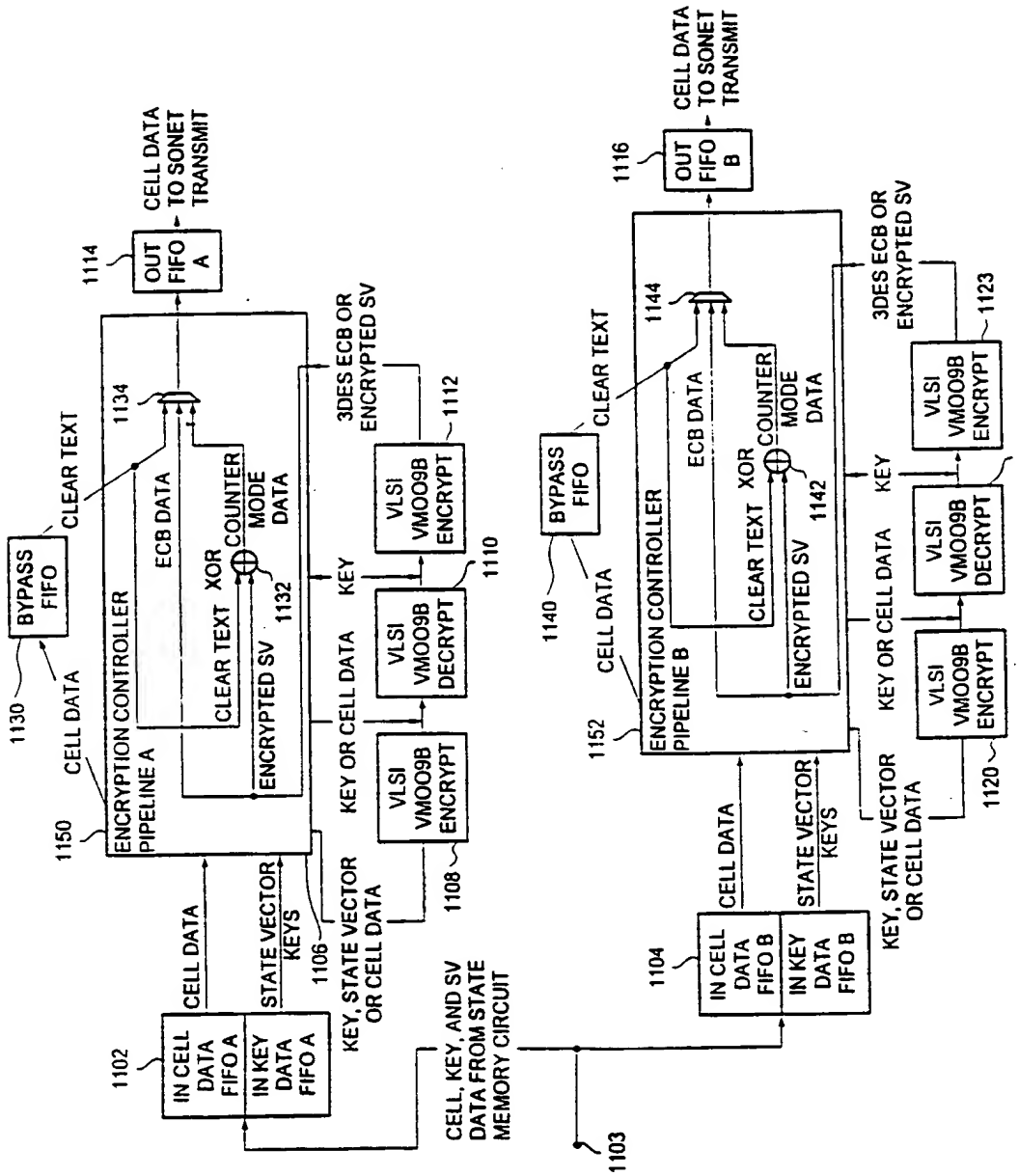


FIG. 11.

TRIPLE DES ENCRYPTION CIRCUIT

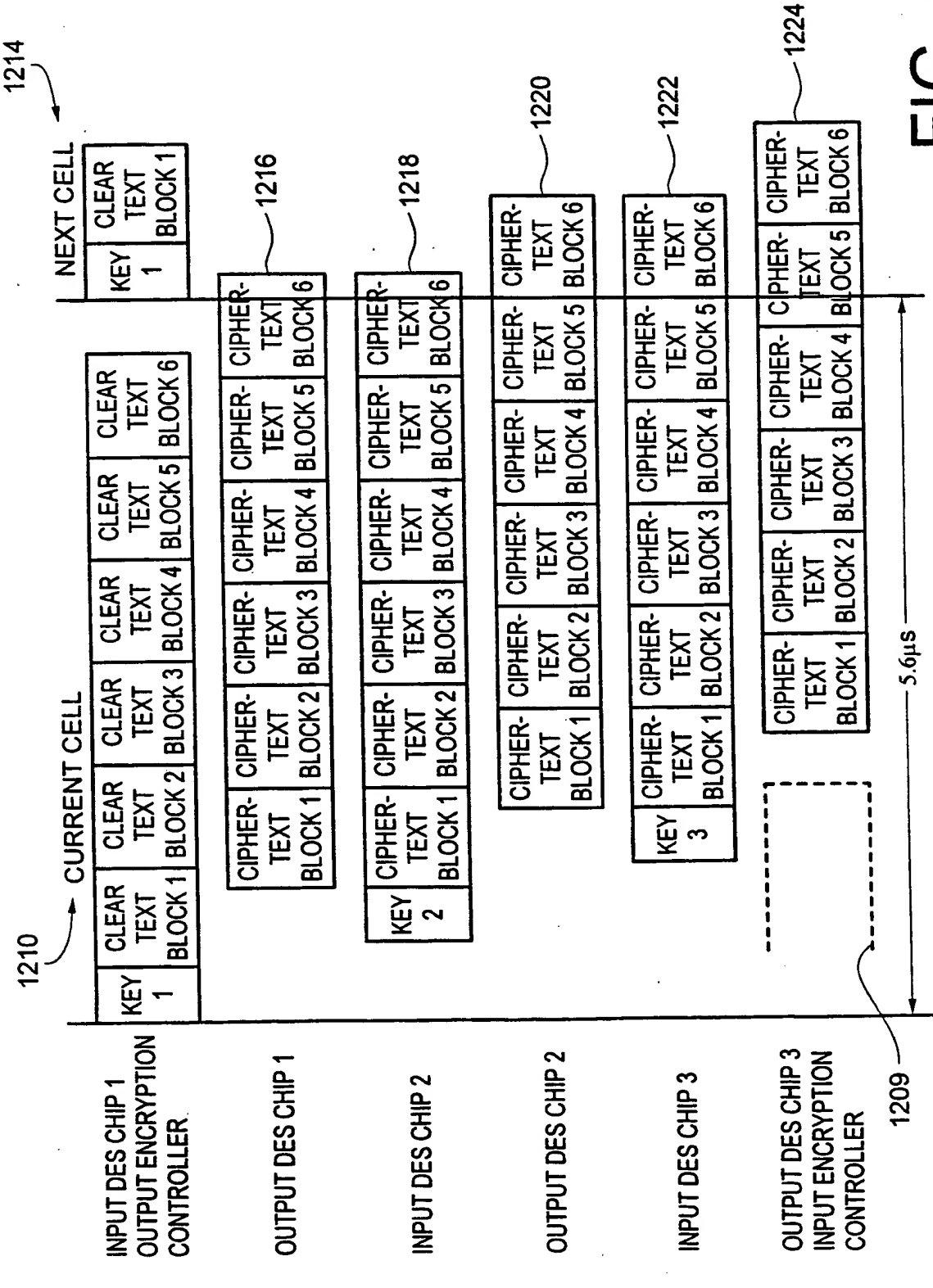


FIG. 12

TIMING FOR DATA I/O FOR TRIPLE DES CIRCUIT

INTERNATIONAL SEARCH REPORT

Inte ,onal Application No
PCT/US 98/19096

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 H04Q11/04

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 H04Q H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 0 673 133 A (NEDERLAND PTT) 20 September 1995 see column 1, line 42 - column 2, line 25 see column 4, line 15 - column 6, line 37 see column 10, line 3 - line 57 ---	1,5-7, 10, 14-16, 24,27, 30,31, 33,36, 37,39,40
A	WO 96 33564 A (SECURE COMPUTING CORP) 24 October 1996 see page 4, line 19 - page 6, line 18 see page 9, line 16 - line 19 --- -/--	1,10,19, 24,27, 30,33, 36,39

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
2 February 1999	15/02/1999

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl. Fax: (+31-70) 340-3016	Gregori, S

1

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US 98/19096

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 652 661 A (AT & T CORP) 10 May 1995 see column 7, line 17 - column 8, line 34; figure 4	1-41
A	STEVENSON D ET AL: "DESIGN OF A KEY AGILE CRYPTOGRAPHIC SYSTEM FOR OC-12C RATE ATM" PROCEEDINGS OF THE SYMPOSIUM ON NETWORK AND DISTRIBUTED SYSTEM SECURITY, 16 February 1995, pages 17-30, XP000617110 * sections 2.1, 4.2, 6.1 * see figure 2	1-41

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

Inte: onal Application No
PCT/US 98/19096

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0673133 A	20-09-1995	NL 9400428 A	01-11-1995
		CA 2144831 A,C	19-09-1995
		US 5809147 A	15-09-1998
WO 9633564 A	24-10-1996	US 5796836 A	18-08-1998
		AU 5542896 A	07-11-1996
		EP 0821853 A	04-02-1998
		JP 10508450 T	18-08-1998
EP 0652661 A	10-05-1995	US 5473696 A	05-12-1995
		JP 7193566 A	28-07-1995

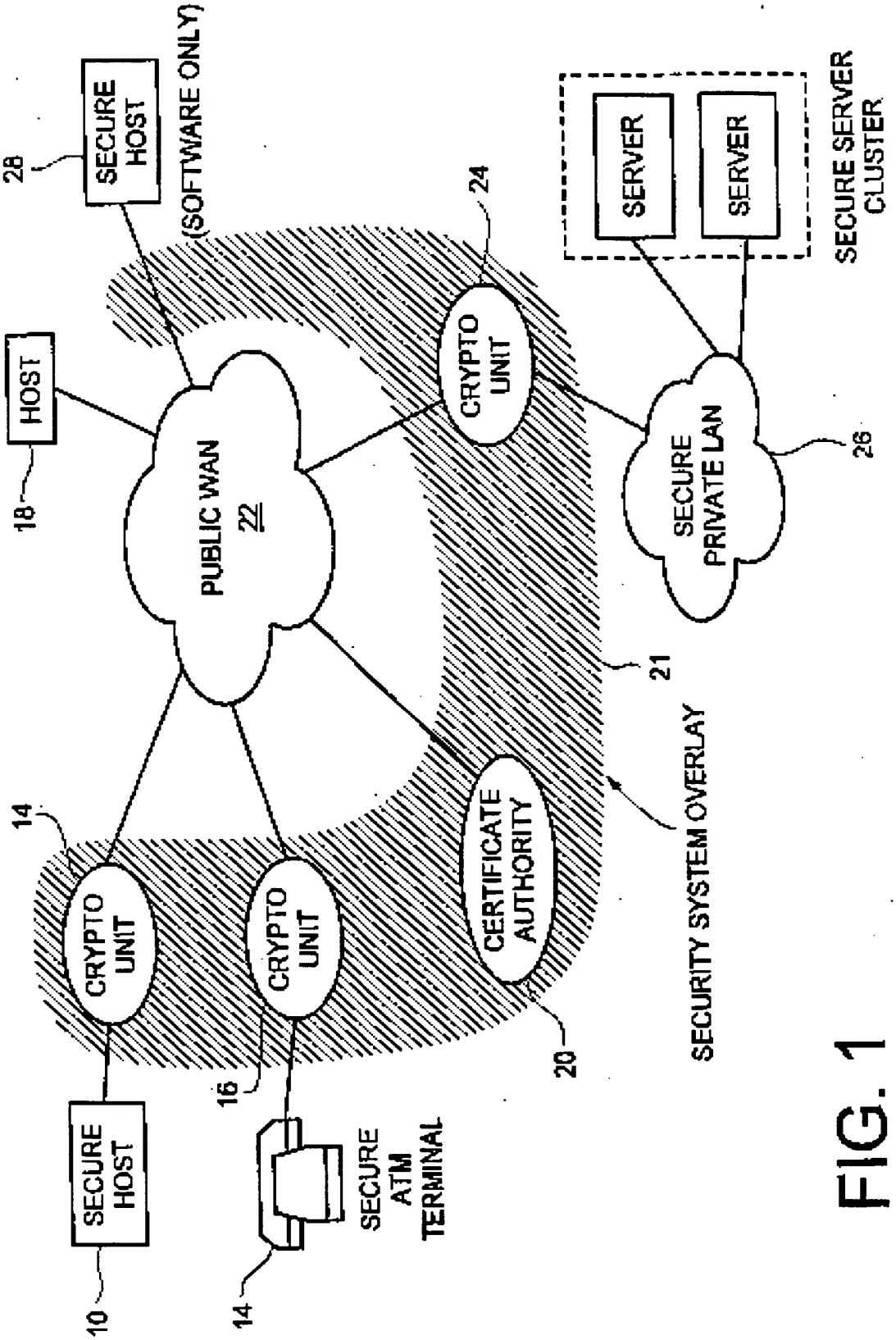


FIG. 1

FIG. 2

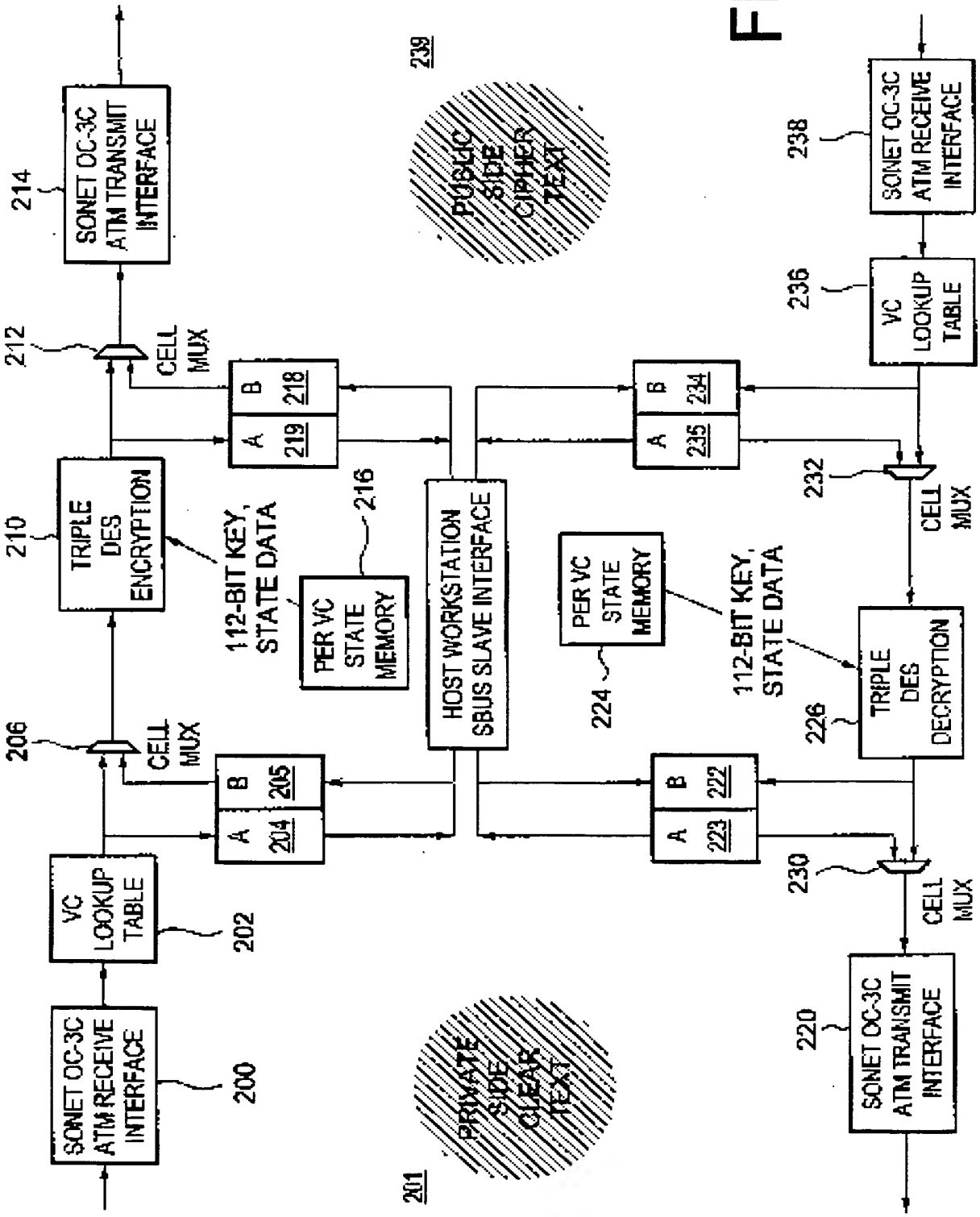
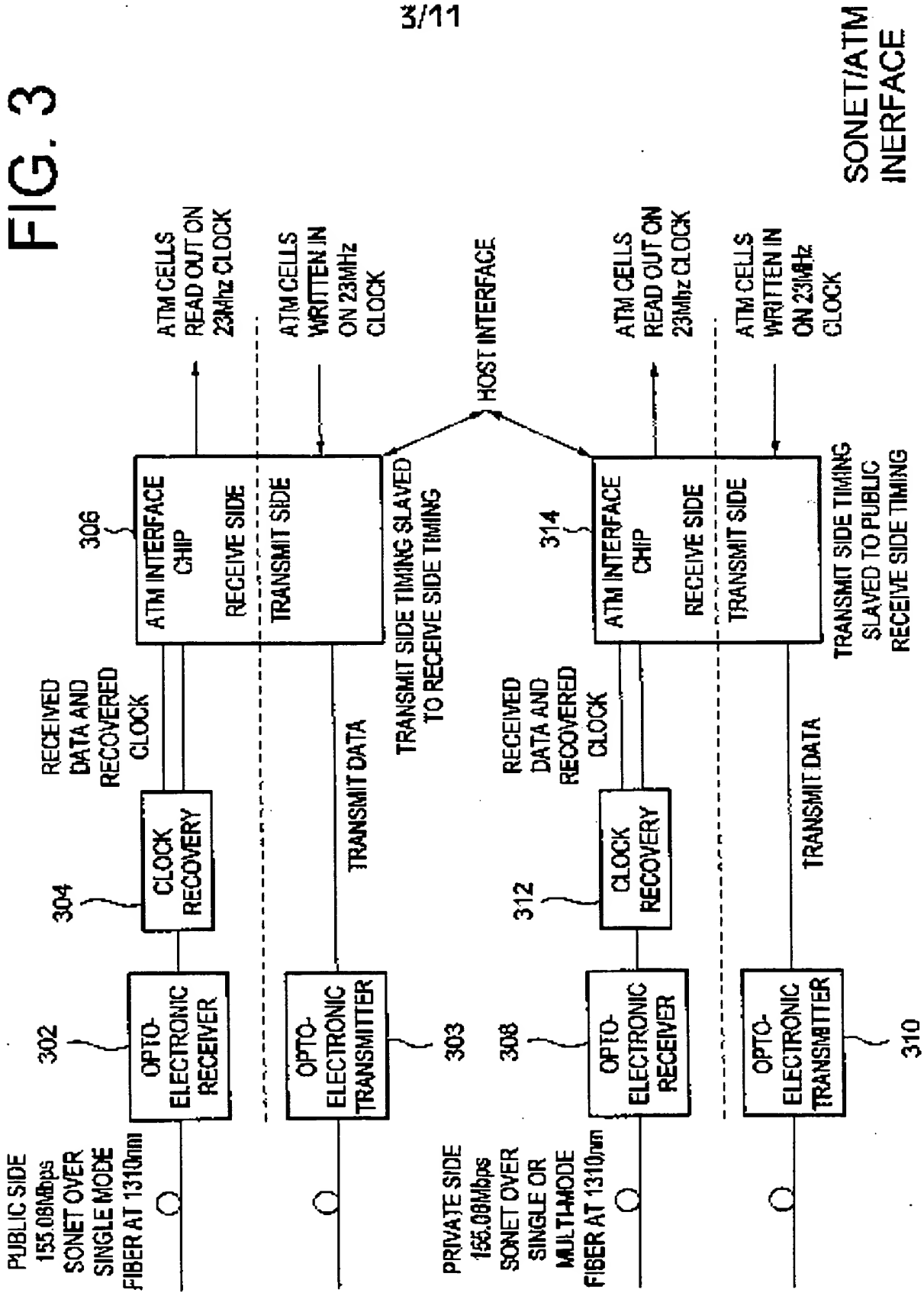


FIG. 3



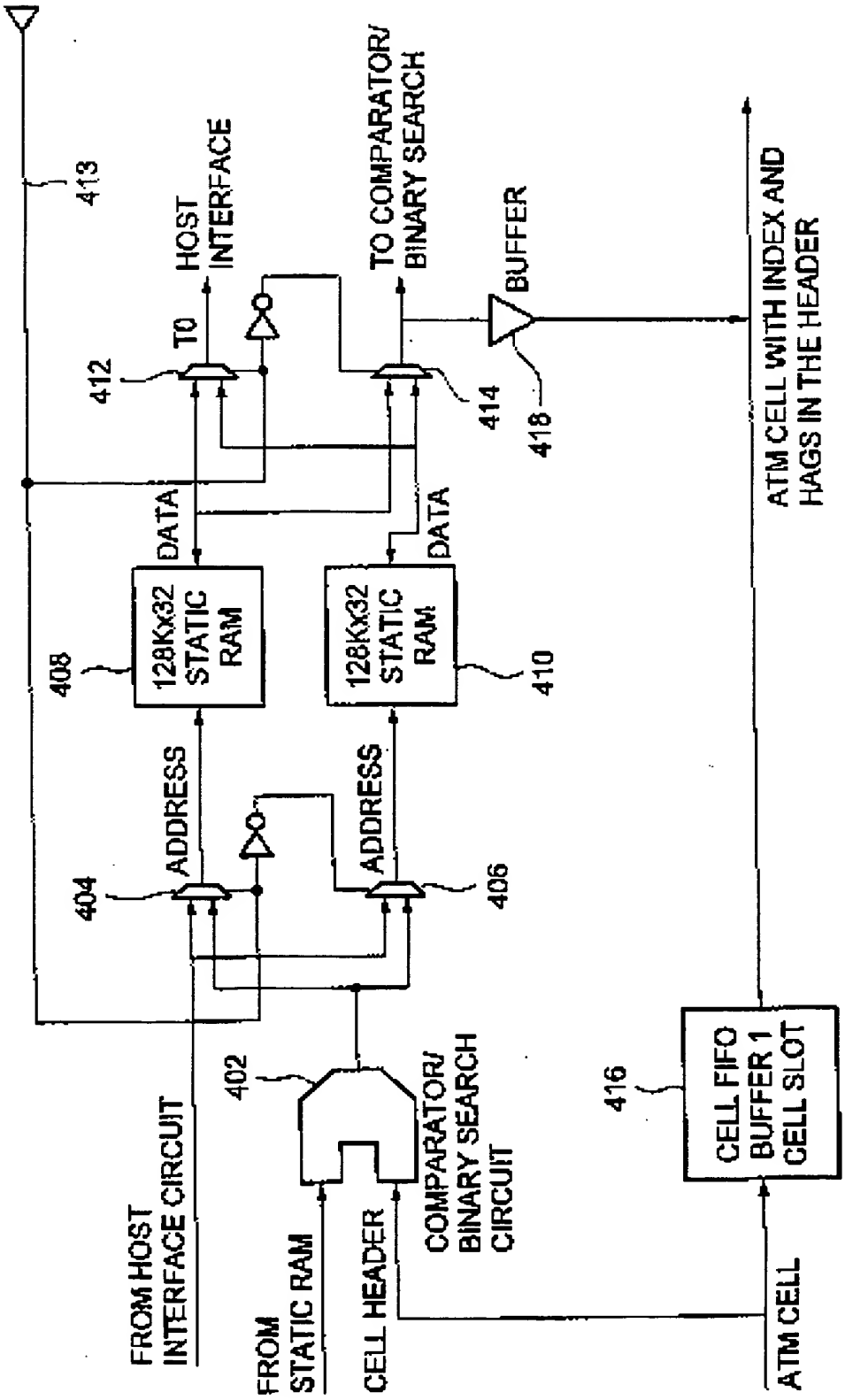
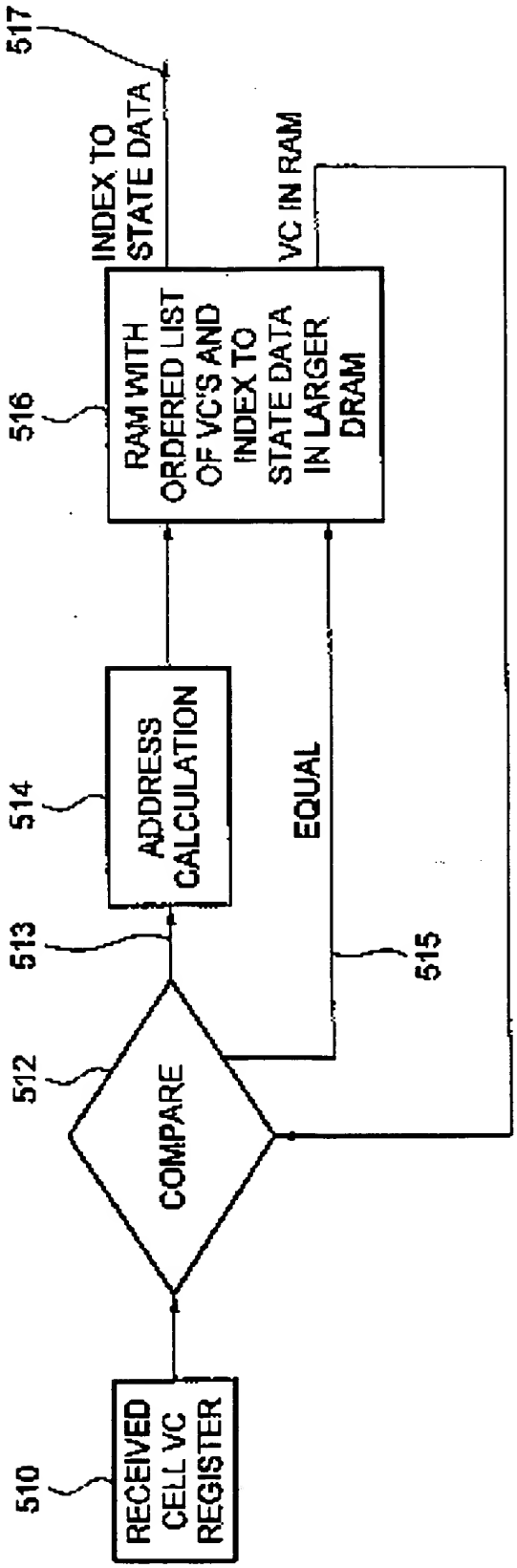
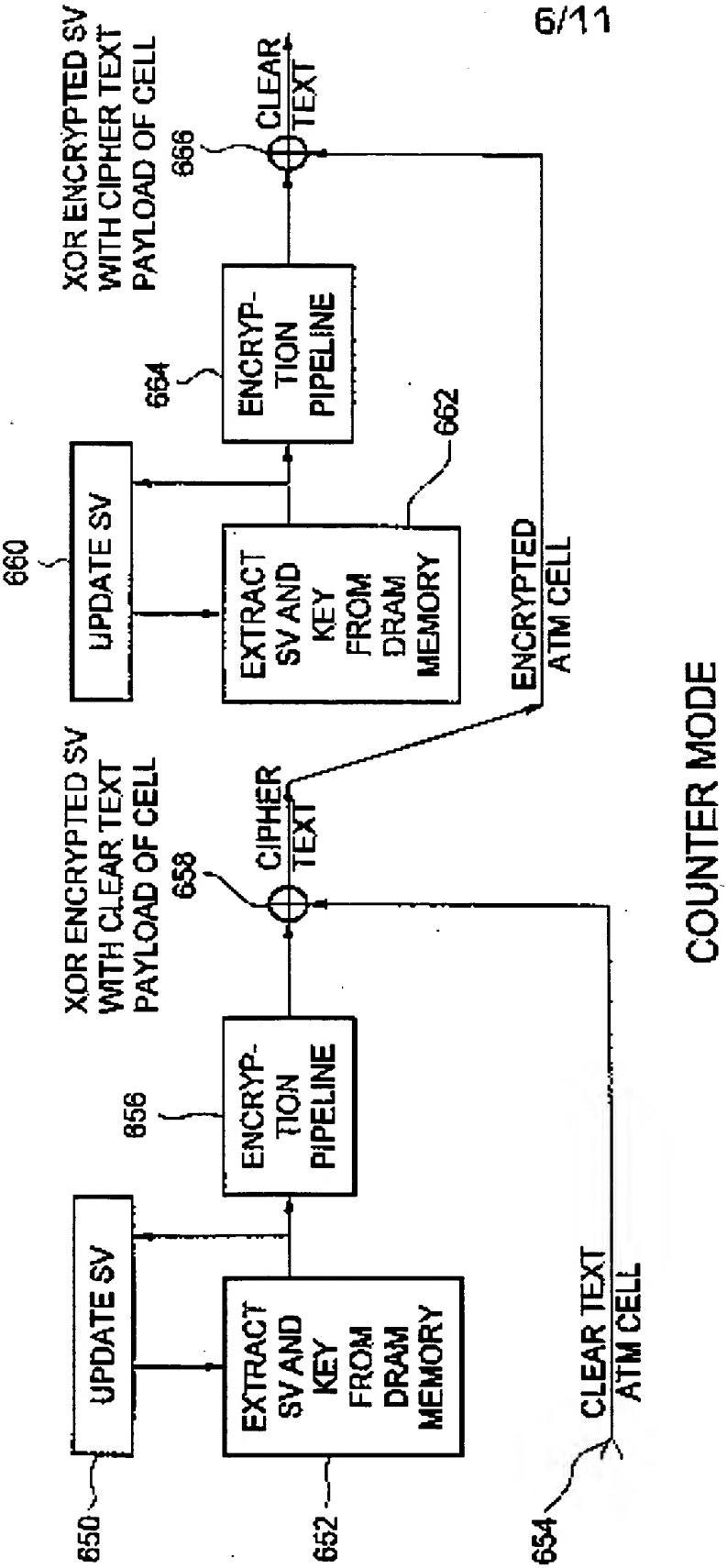


FIG. 4



VC LOOKUP

FIG. 5



COUNTER MODE

FIG. 6

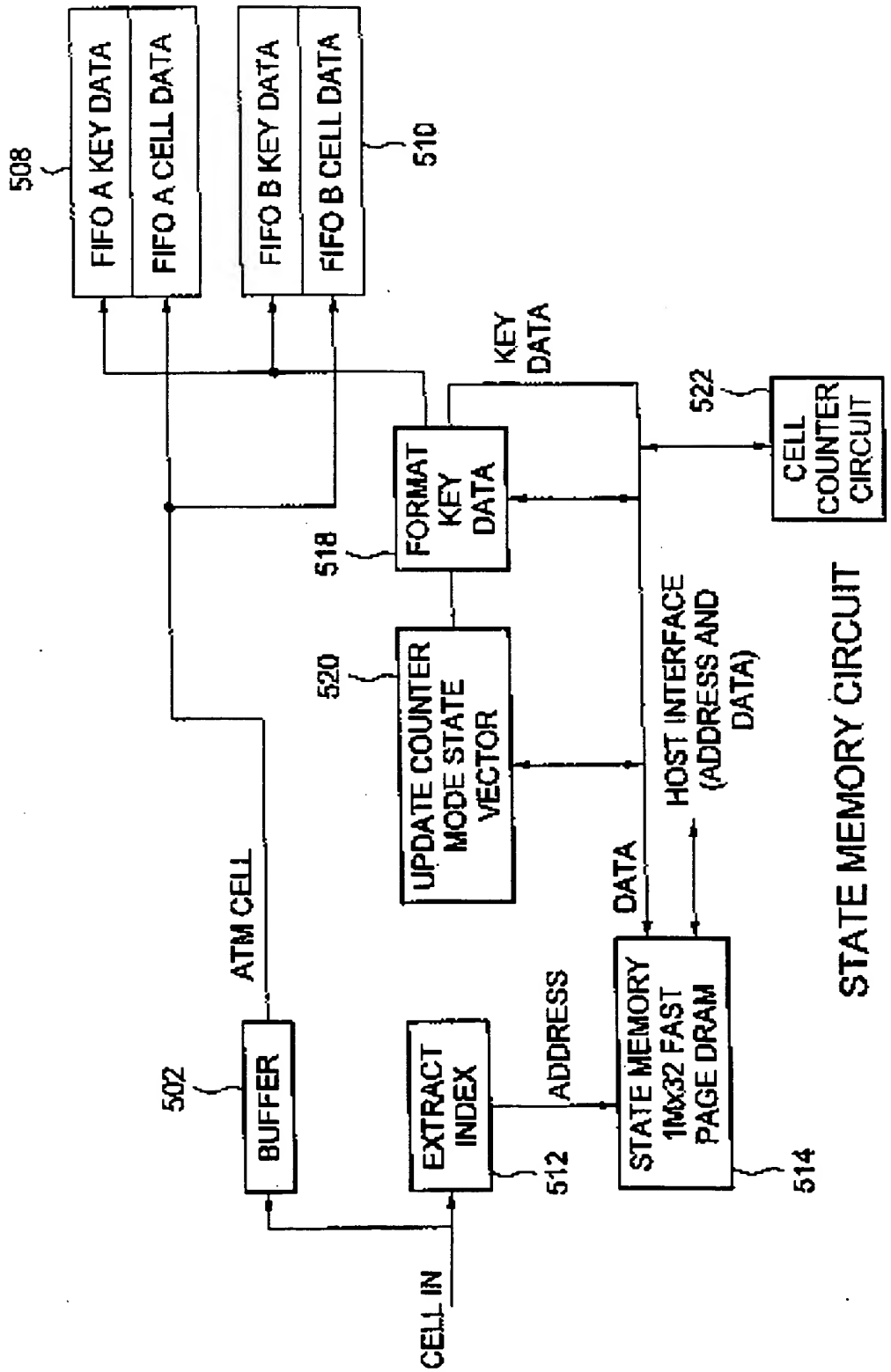
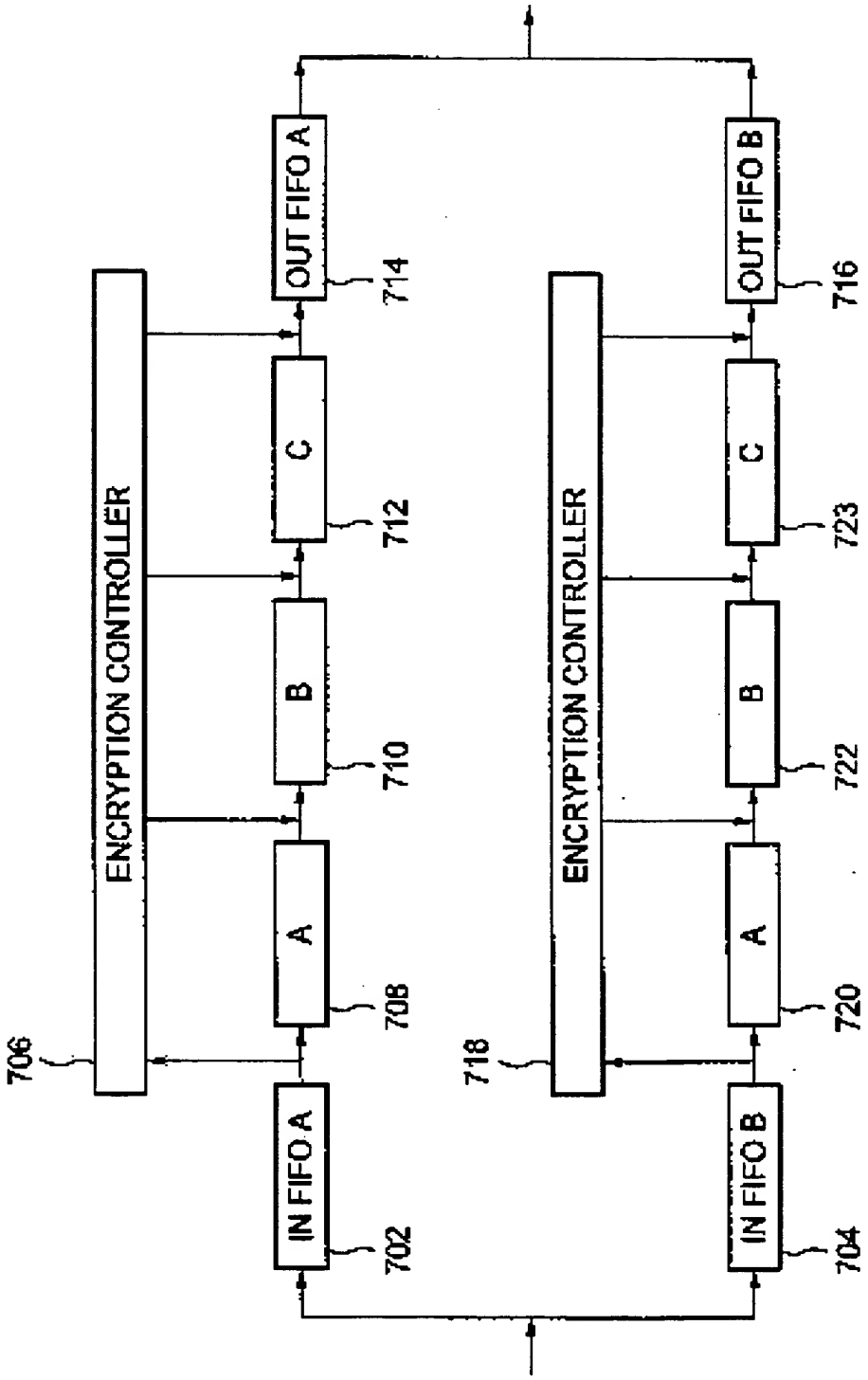


FIG. 7



TRIPLE DES ENCRYPTION

FIG. 8

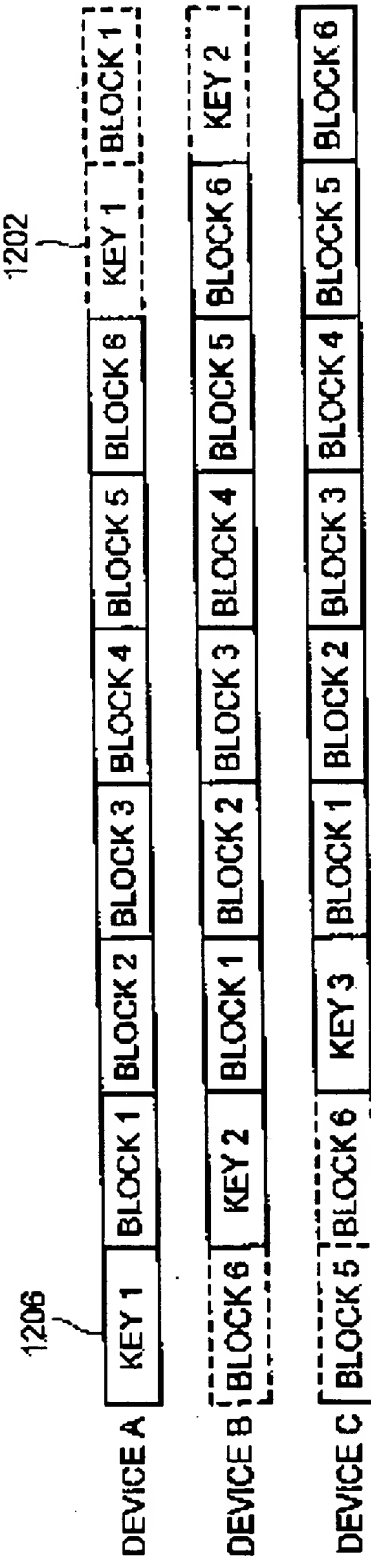


FIG. 9

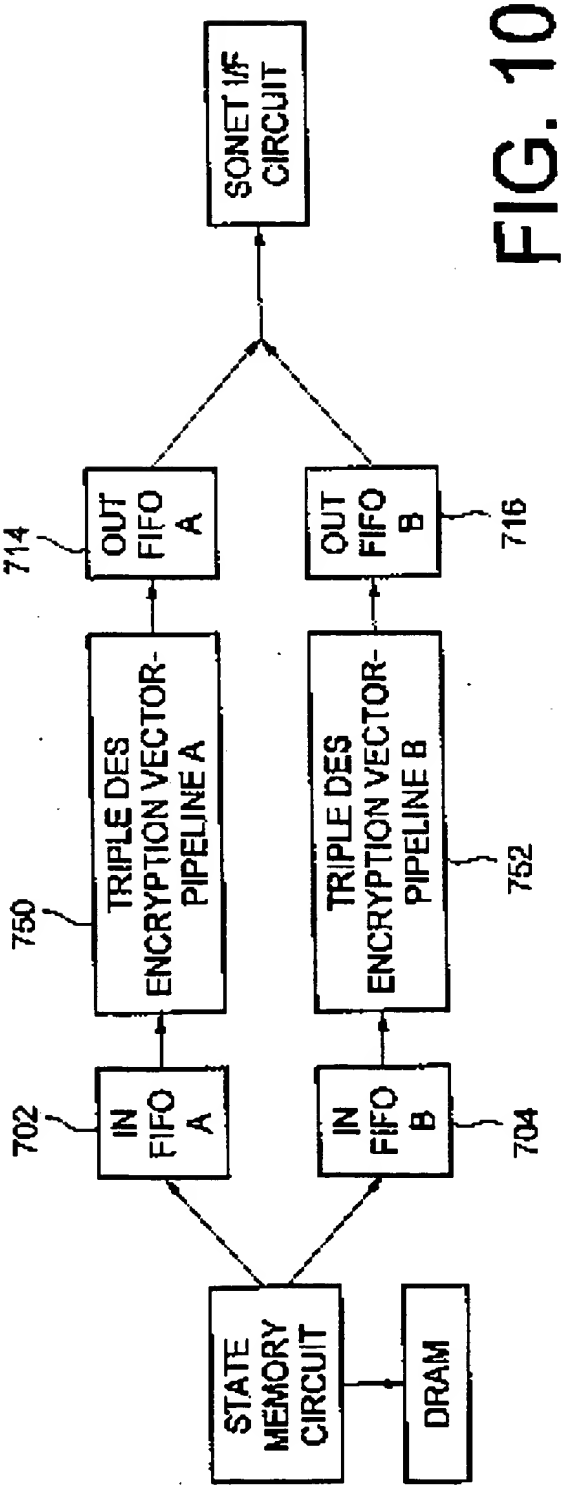


FIG. 10

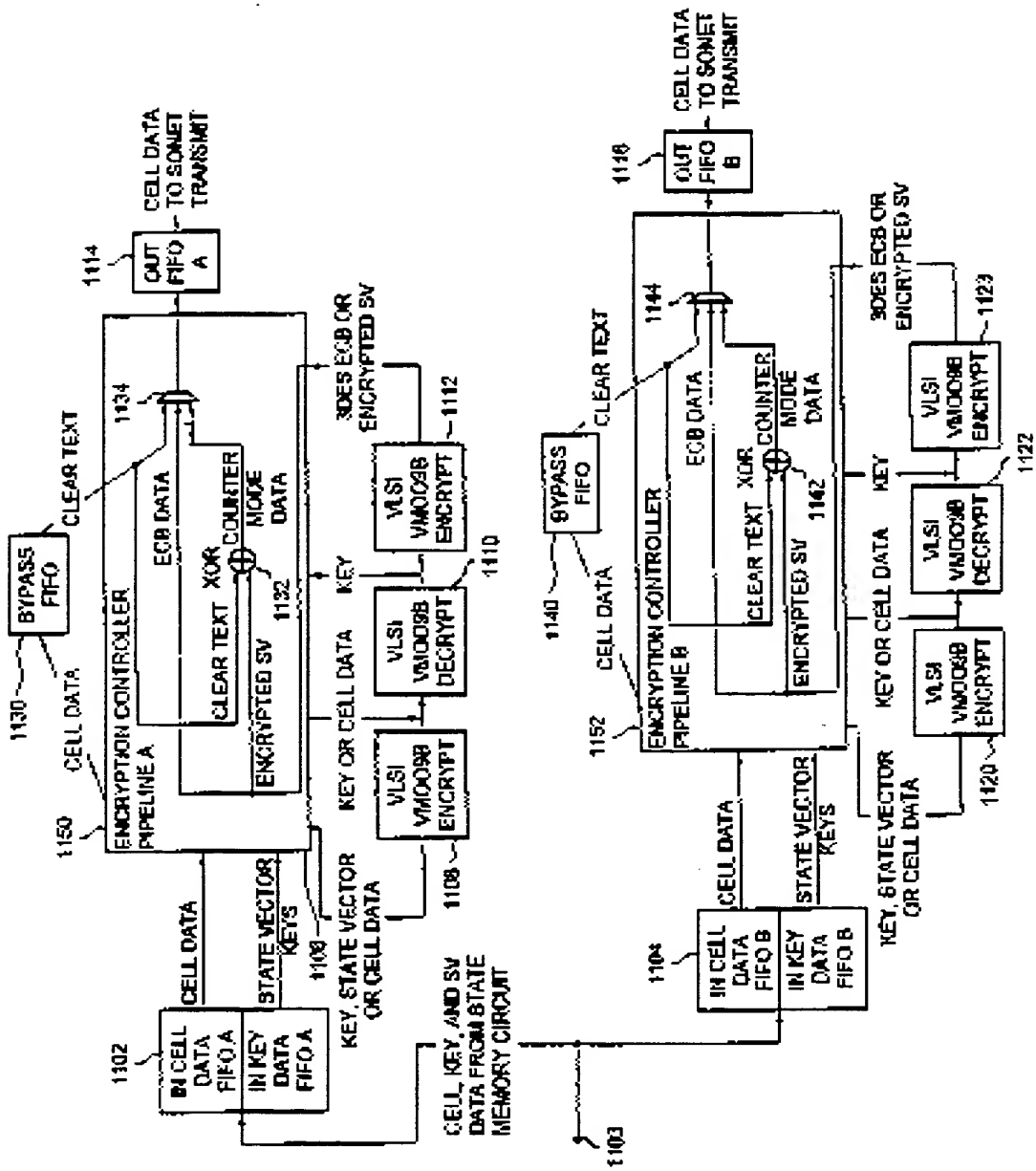


FIG. 11

TRIPLE DES ENCRYPTION CIRCUIT

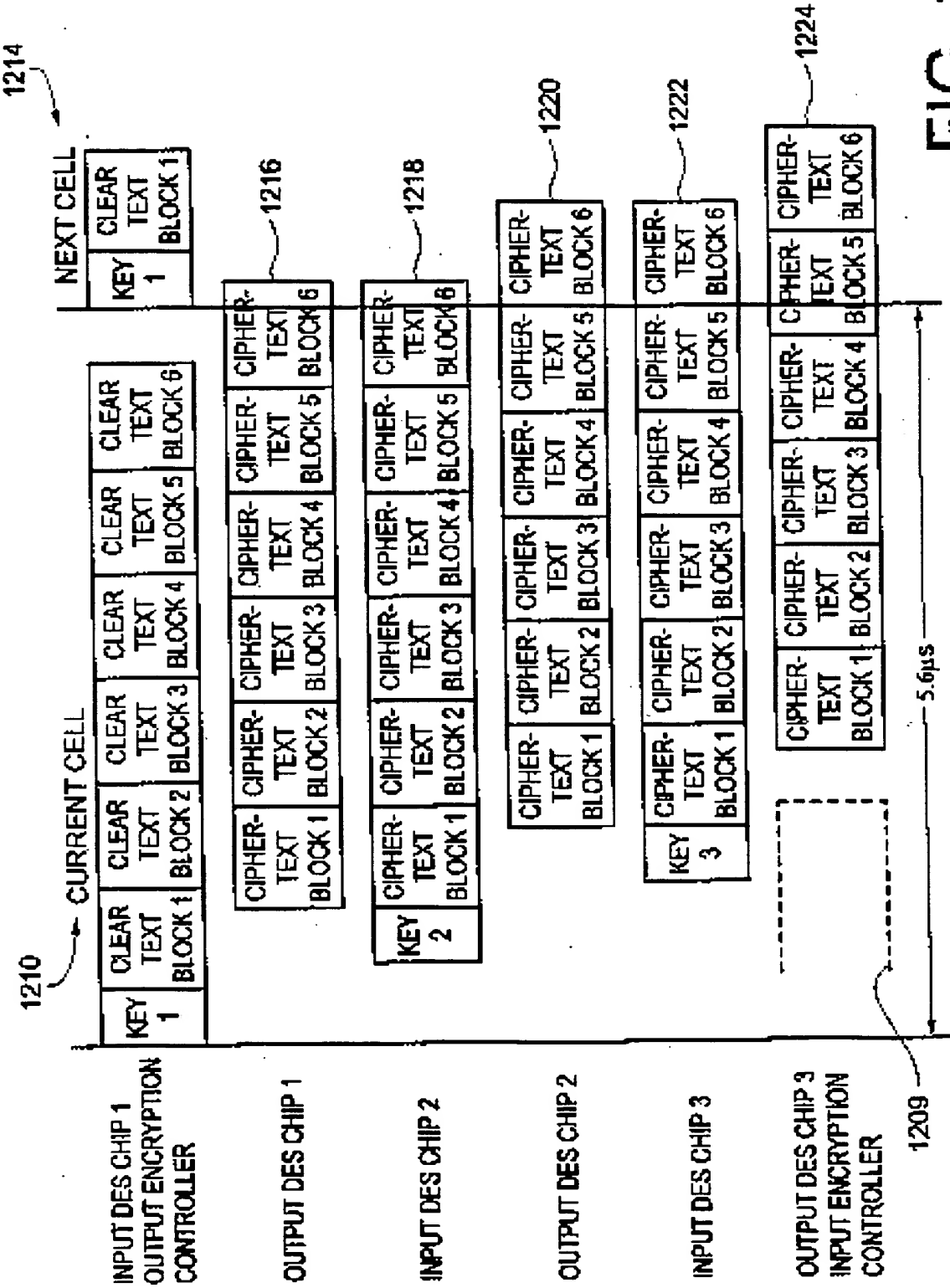


FIG. 12

TIMING FOR DATA I/O FOR TRIPLE DES CIRCUIT